ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

IMSI CATCHER TESPİT YÖNTEMLERİ TASARIMI VE UYGULAMASI

Ömer Faruk ÇELİK

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2015

TEZ ONAYI

Ömer Faruk ÇELİK tarafından hazırlanan **"IMSI Catcher Tespit Yöntemleri Tasarımı ve Uygulaması"** adlı tez çalışması 29/01/2015 tarihinde aşağıdaki jüri tarafından oy çokluğu/birliği ile Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. Refik SAMET
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Jüri Üyeleri :
Başkan :

Üye :

Üye :

Yukarıdaki sonucu onaylarım.

Prof. Dr. İbrahim DEMİR
Enstitü Müdürü

ETİK

Ankara Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

29/01/2015

Ömer Faruk ÇELİK

ÖZET

Yüksek Lisans Tezi

IMSI CATCHER TESPİT YÖNTEMLERİ TASARIMI VE UYGULAMASI

Ömer Faruk ÇELİK

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman : Doç. Dr. Refik SAMET

GSM, mobil terminaller tarafından kullanılan ve standartları Avrupa Telekomünikasyon Standartları Enstitüsü tarafından belirlenen ikinci nesil hücresel ağ standardıdır. GSM, 25 yıllık bir teknoloji olmasına rağmen %90 market payı ile dünyada en yaygın kullanılan mobil iletişim sistemi olup, 219 ülke ve bölgede kullanılmaktadır. GSM'in yaygın kullanımına rağmen GSM'e ait güvenlik sorunları devam etmekte ve bu açıklar bilgi güvenliğini önemli ölçüde tehdit etmektedir. Söz konusu güvenlik açıkları arasında uçtan uca kriptolamanın bulunmaması, mobil terminal ile baz istasyonu arasında bulunan hava arayüzündeki kripto zafiyeti ve mobil terminal ve baz istasyonu arasında karşılıklı doğrulamanın olmaması öne çıkmaktadır. Mobil terminal ve baz istasyonu arasında karşılıklı doğrulamanın olmaması, ortadaki adam (man-in-the-middle) saldırılarına kapı aralamakta ve baz istasyonları ve mobil terminallerin saldırıya uğramasına neden olmaktadır. Ayrıca söz konusu saldırı ile mobil terminalin kimliğinin çalınması, tele kulak, mobil terminal ve baz istasyonu sahteciliği ve diğer ortadaki adam saldırıları sahte baz istasyonları kullanılarak gerçekleştirilebilmektedir. Bu sebeple sahte baz istasyonu saldırılarının tespit edilmesi ve kullanıcıların, operatörlerin ve hatta güvenlik güçlerinin bu saldırılardan haberdar edilmesi oldukça önemlidir. Yapılan çalışmada öncelikle sahte baz istasyonu saldırıları konusunda literatür taraması yapılıp, bahse konu saldırılar analiz edilmiş olup, bu saldırıların tespit edilmesine yönelik bir algoritma geliştirilmiştir. Ayrıca, gerçek veriler kullanılarak simülasyon yapılıp, sahte baz istasyonu saldırılarının geliştirilen algoritma ile tespit edilebilirliği gösterilmiştir.

Ocak 2015, 63 sayfa

Anahtar Kelimeler: GSM güvenliği, sahte baz istasyonu saldırıları, saldırı tespiti, ortadaki adam saldırıları.

ABSTRACT

M.Sc. Thesis

DESIGN AND IMPLEMENTATİON OF METHODS FOR DETECTING ACTIVE IMSI CATCHER

Ömer Faruk ÇELİK

Ankara University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Supervisor : Assoc.Prof. Dr. Refik SAMET

GSM, is a standard developed by European Telecommunications Standards Institute. GSM is second generation digital network protocols and developed for mobile terminals. Although GSM is 25 years old technology, it has 90% market share and is available in 219 territories. GSM has some security problems despite the common usage and these security problems seriously threaten information security. Deficiency of end-to-end encryption, weak encryption in air interface between mobile terminal and base station, lack of mutual authentication between base station and mobile terminal are the best known security leaks of GSM. Lack of mutual authentication between base station and mobile terminal causes man-in-the middle attacks and also causes various attacks targeting mobile stations and base stations. In addition, by using fake bts attacks, attackers can get mobile terminal identity, eavesdropping, impersonation of mobile terminal and base station and other types of man-in-the-middle attacks. Therefore, detection of fake bts attacks then warning mobile terminal users, GSM operators and even security forces would be pretty important. In this work, literature review about fake bts attacks has been done and fake bts attacks are analyzed. Then, fake bts attack detection algorithm is developed. Besides, by the help of proposed algorithm, feasibility of fake base station attack detection, has been shown by simulation which is based on real GSM network values.

January 2015, 63 pages

Key Words : GSM security, fake base station attacks, attack detection, man-in-the-middle attacks.

TEŞEKKÜR

Bu tez çalışmasının planlanmasında, araştırılmasında, yürütülmesinde ve oluşturulmasında ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren ve akademik ortamda olduğu kadar insani ilişkilerde de engin fikirleriyle yetişme ve gelişmeme katkıda bulunan Bilgisayar Mühendisliği bölümünde görevli danışman hocam sayın Doç.Dr. Refik SAMET'e sonsuz teşekkürlerimi sunarım.

Sevgili eşime ve aileme manevi hiçbir yardımlarını esirgemeden yanımda oldukları için tüm kalbimle teşekkür ederim.

Ömer Faruk ÇELİK
Ankara, Ocak 2015

İÇİNDEKİLER

SİMGELER DİZİNİ

<>	Eşit değil
>	Büyük
<	Küçük
≥	Büyük veya eşit
≤	Küçük veya eşit
dBm	Bir miliwatt'a göre desibel orani

Kısaltmalar

2G	İkinci jenerasyon
3G	Üçüncü jenerasyon
3GPP	3G ortaklık programı
A5/1/2/3	Kriptoloma algoritmaları
AGCH	Erişim kanalı
AUC	Doğrulama merkezi
BCH	Yayın kanalı
BCCH	Yayın kontrol kanalı
BSC	Baz istasyonu kontrolörü
BSS	Baz istasyonu alt sistemleri
BTS	Baz istasyonu
C1	Hücre seçim parametresi
C2	Hücre yeniden seçim parametresi
CCCH	Ortak kontrol kanalı
CELLID	Hücre tanımlama numarası
CKSN	Şifreleme sıra numarası
DCCH	Atanmış kontrol kanalı
DCS	Dijital hücresel sistem
DTMF	Çift tonlu çoklu frekanslı sinyalizasyon
EIR	Cihaz kimlik merkezi
FACCH	Hızlı ilişkili kontrol kanalı

FCCH	Frekans düzeltme kanalı
FDMA	Frekans bölümlü çoklu erişim
GMSK	Gaus modülasyon anahtar kaydırma
GPS	Küresel konumlama sistemi
GSM	Mobil iletişim için küresel sistem
G-MSC	Ağ alt geçidi mobil santrali
HLR	Dahili kayıt merkezi
HSDPA	Yüksek hızda veri paketi indirme bağlantıs
IMEI	Tekil mobil cihaz numarası
IMSI	Tekil abone numarası
ISDN	Bütünleştirilmiş sayısal ağ hizmetleri
ITU	Uluslararası Telekomünikasyon Birliği
LAI	Lokasyon alanı değeri
LMSI	Yerel abone numarası
LTE	Dördüncü jenerasyon iletişim protokollerinden birisi
MC	Mobil cihaz
MM	Mobil yönetim
MT	Mobil terminal (SIM Kart ve Mobil Cihaz)
MCC	Mobil ülke kodu
MCKS	Mobil cihaz kontrol merkezi
MSC	Mobil santral
MNC	Mobil operatör kodu
MSISDN	Abone tanımlama numarası
MSRN	Mobil terminal dolaşım numarası
NCC	Ağ renk kodu
NSS	Ağ alt sistemleri
OSI	Açık iletişim sistemi
OSS	Operasyon merkezi alt sistemleri
PCS	Kişisel iletişim sistemi
PLMN	Kablosuz kamu iletişim ağı
PIN	Kişisel doğrulama numarası
PSTN	Anahtarlanmış kamu telefon ağı

PUK	PIN bloke kaldırma numarası
RACH	Rastgele erişim kanalı
SCH	Senkronizasyon kanalı
SACCH	Yavasş ilişkili kontrol kanalı
SDCCH	Ayrık atanmış kontrol kanalı
SIM	Abone kimlik modülü
SMS	Kısa mesaj servisi
T3212	Lokasyon güncelleme zamanlayısı
TMSI	Geçici abone numarası
TCE	Terminal kontrol elementi
TCH	Trafik kanalı
TCH/F	Tam-oranlı trafik kanalı
TCH/H	Yarı oranlı trafik kanalı
TDMA	Zaman bölümlü çoklu erişim
TRAU	Sıkıştırma ünitesi
UMTS	3. Jenerasyon hücresel ağ çeşidi
VLR	Ziyaretçi kayıt merkezi

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

1.1 Tez Konusu, Amacı ve Önemi

Mobil İletişim için Küresel Sistem (Global System for Mobile Communication - GSM), %90 market payı ile dünyada en yaygın kullanılan mobil iletişim sistemi olup, 219 ülke ve bölgede kullanılmaktadır. Avrupa tarafından geliştirilmiş olan GSM, Dünya tarafından kabul görmüş olup, Uluslararası Telekomünikasyon Birliğinin (International Telecommunication Union - ITU) yaptığı araştırmaya göre 2008 yılı sonunda Dünya geneli İnternet kullanan insan sayısı 1,5 milyar iken, 4,1 milyar GSM aboneliği bulunmaktaydı. 2013 yılı sonlarında ise GSM aboneliği sayısı neredeyse 7 milyara ulaşmıştır. 25 yıllık bir teknoloji için bu büyük bir başarıdır. Bununla birlikte, GSM'in yaygın olarak kullanılan bir iletişim protokolü olduğu açıktır ve bu sebeple GSM güvenliği oldukça önemlidir (Anonymous 2014a), (Anonymous 2014b) .

GSM teknolojisinin güvenliği, GSM'in kullanılmaya başlandığı andan itibaren araştırmacıların ilgi odağında olmuştur. Ancak, GSM'in güvenlik problemleri hala devam etmektedir (Vales-Alonso vd. 1999), (Ntantigian ve Xenakis 2011), (Ahmadian 2010). Bu problemlerden en önemlileri;

1) Uçtan uca kriptolama kullanılmaması: Kriptolamanın yalnız Mobil Terminal (MT) ile Baz İstasyonu (BTS) arasında olması,
2) Büyük gökkuşağı tabloları (rainbow tables) ile saldırılabilen GSM hava arayüzündeki (air-um interface) kripto zafiyeti: MT ve BTS arasında bulunan kriptolamanın kırılabilir olması (Kalenderi vd. 2012),
3) MT ve BTS arasında karşılıklı doğrulamanın olmaması: BTS'in, MT'nin kimliğini ve yetkisini kontrol edebilmesi, fakat MT'nin, BTS'inkini kontrol edememesidir.

Karşılıklı doğrulama eksikliğini kullanarak tele kulak, MT kimliği çalınması ve seçici yakalama (selective interceptor) saldırıları gibi çeşitli IMSI Catcher (sahte BTS) saldırıları yapılabilmektedir. Sahte BTS saldırıları MT kimliği çalma gibi nispeten

tehlikesiz olabileceği gibi insansız hava araçlarının sahte BTS saldırısı kullanarak MT'nin coğrafi konumunu belirleyip hava saldırısı yapması gibi ölümcül alanlarda da kullanılabilmektedir (Scahill J ve Greenwald 2014). Bu çalışmada, GSM'in karşılıklı doğrulama zafiyeti ve bu zafiyeti istismar eden sahte baz istasyonu saldırıları ele alınacaktır.

Konu ile ilgili literatürde sahte BTS saldırılarının nasıl gerçekleştirileceğine dair çeşitli çalışmalar olmasına rağmen, sahte BTS saldırılarının tespit edilip kullanıcının uyarılmasına yönelik pek bir çalışmaya rastlanılmamıştır. Bu nedenle, sahte BTS saldırılarına karşı önlemlerin geliştirilmesi ve MT kullanıcısının sahte BTS ataklarına karşı uyarılması önem arz etmektedir. Bu çalışmayla, sahte BTS saldırı teknikleri analiz edilmekte ve bu saldırıların tespit edilmesine yönelik bir algoritma önerilmektedir.

Bölüm 1'de tez konusunun tanıtımı yapılmış, tezin öneminden bahsedilmiş, GSM tarihçesi ve GSM mimarisinden bahsedilmiştir. Bölüm 2'de sahte baz istasyonu saldırıları ile ilgili çalışmalar incelenmiştir. Bölüm 3'de ilgili GSM protokollerinin analizi yapılmış ve sahte BTS saldırı tespit algoritması önerilmiştir. Bölüm 4'de, sahte BTS algoritmasının simülasyonu yapılmıştır. Beşinci bölümde ise sonuç ve değerlendirmelere yer verilmiştir.

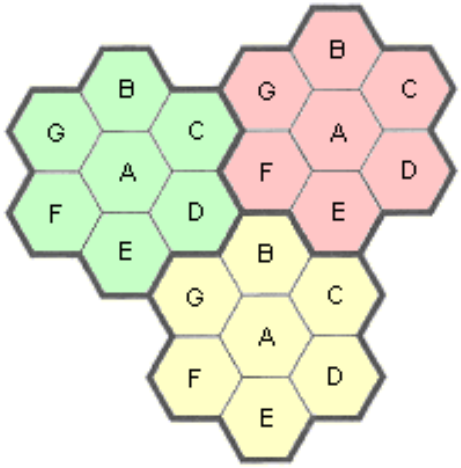
1.2 GSM Tarihçesi

GSM kısaltması ilk olarak 1982 yılında Groupe Special Mobile'ın kısaltması olarak kullanılmıştır. GSM projesi 900 MHz'de çalışacak yeni bir mobil iletişim standardı geliştirmek için başlatılmış ve geliştirilen dijital teknloji birinci jenerasyon (1G) analog sistemin yerini alıp ikinci jenerasyon (2G) olarak adlandırılmıştır. 1991 yılında GSM ilk olarak son kullanıcıya yönelik denenmiş ve aynı yıl GSM, Global System for Mobile Communication'ın kısaltması olarak kullanılmaya başlanmıştır. Yine 1991 yılında GSM 'in 1800 MHz'de çalışan ilk türevi DCS 1800 (Digital Cellular System 1800) ortaya çıkmıştır. Amerika Birleşik Devletlerinde 'DCS 1800' 1900 MHz'e uyarlanıp PCS 1900 (Personal Communication System 1900) olarak kullanılmaya başlanmıştır (Anonymous 2014c).

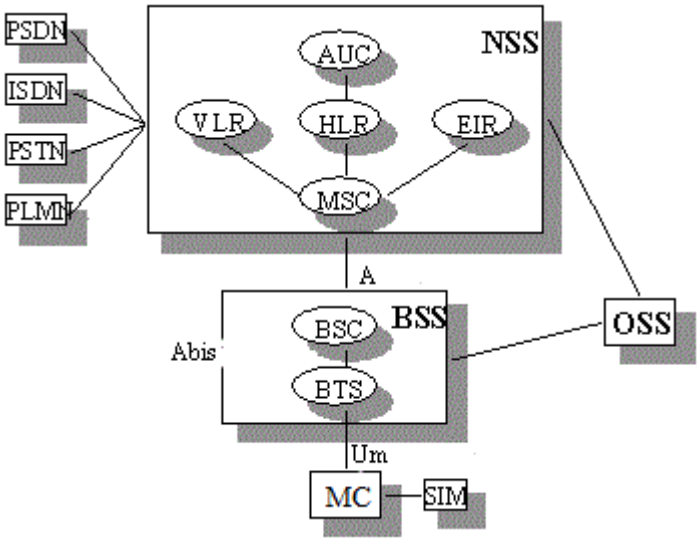
1992 yılında, ilk ticari GSM ağları hizmet vermeye başlamış ve ilk taşınabilir mobil terminaller kullanıma sunulmuştur, 1993 yılında ise GSM kullanıcı sayısı 1 milyon rakamına ulaşmış ve SMS ticari olarak ilk defa kullanılmaya başlanmıştır. 1995 yılnda 60 ülkede 100 GSM ağı 10 milyon kullanıcı tarafından kullanılmaya başlanmıştır. Yine aynı yıl PCS 1900 ABD'de kullanılmaya başlanmış ve fax, data servisleri başlatılıp, GSM üzerinden video aktarımının, gösterimi yapılmıştır. 1997 yılında 100 ülkede 200 GSM ağı 70 milyon kullanıcı tarafından kullanılmaya başlanmıştır. 2000 yılında GSM/UMTS üçüncü jenerasyon (3G) standartları 3GPP tarafından yayınlanmış olup 2002 yılında GSM/UMTS (HSDPA) (3.5 G olarak da bilinen) standartlar yayınlanmıştır. 2003 yılında dünya çapında 1 milyar kullanıcıya ulaşılmıştır. 2009 yılında 4 milyar kullanıcıya erişilmiş ve ilk LTE (4G – 4. jenerasyon) denemeleri yapılmış olup 2013 yılı sonunda GSM aboneliği sayısı 7 milyara yaklaşmıştır (Anonymous 2014b).

1.3 GSM Mimarisi

Tüm modern mobil ağlarda olduğu gibi GSM de şekil 1.1 de gösterildiği gibi hücresel yapı kullanmaktadır. Bu yapının kullanılmasındaki temel fikir, kullanılabilir frekansı baz istasyonları arasında dağıtmak ve bir bölgede kullanılan frekansı farklı bölgelerde tekrar kullanabilmektir. Ayrıca şekil 1.2'de genel hatlarıyla gsöterilen GSM mimarisi de ileriki bölümlerde detaylandırılacaktır.



Şekil 1.1 Hücresel radyo kapsama alanı (Anonymous 2014d)

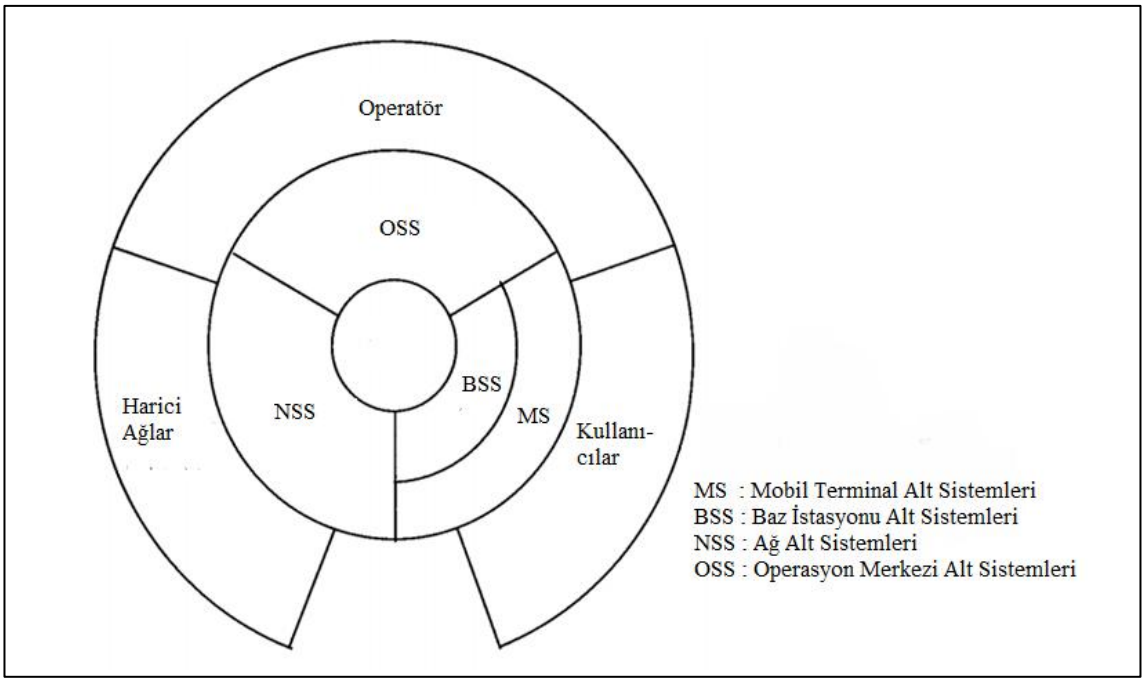


Şekil 1.2 GSM mimarisi

GSM gibi detaylı bir iletişim protokolünü ikiye ayırmak mümkündür. Bunlardan ilki GSM alt sistemleri, diğeri ise GSM arayüzleridir.

1.3.1 GSM alt sistemleri

GSM desteklenebilmesi ve hizmet verebilmesi için çeşitli fonksiyonlara ihtiyaç duymaktadır. GSM'in alt sistemlerinin basit bir hali ve birbirlerine göre konumu şekil 1.3'de gösterilmektedir. Bunlar Mobil Terminal alt sistemleri, Baz İstasyonu alt sistemleri, Ağ alt sistemleri ve Operasyon Merkezi alt sistemleridir (Garg ve Wilkes 1998).



Şekil 1.3 GSM alt sistemleri (Gark ve Wilkes 1998'den değiştirilerek alınmıştır)

1.3.1.1 Mobil terminal alt sistemleri

Mobil cihaz ve SIM, GSM ağına doğrudan erişmek için kullanılan sistem elemanlarıdır.

Abone kimlik modülü (SIM): (Susbcriber Identity Module): SIM GSM abone kaydı sırasında verilen, kullanıcıya ait bilgileri ve kullanıcıya verilecek hizmet tipini saklayan akıllı karttır. Çağrılar mobil cihaz yerine doğrudan SIM'e gelmektedir. SIM'in en önemli görevi veri tutmaktır. SIM'in tuttuğu verilere ait bilgilerden bazıları çizelge 1.1'de gösterilmektedir. GSM'de SIM'in kullanımının sebeplerinden bir tanesi de SIM kullanılarak ilgili GSM veri tabanı ile mobil cihazı birbirinden ayrı tutulabilmektir. Bu şekilde kullanıcı farklı telefonları aynı SIM ile kullanabilmektedir.

Mobil Cihaz: SIM kartlarla beraber kullanıldığında GSM'e erişebilen cihazdır. Baz istasyonu alıcı/verici fonksiyonları mobil cihazda bulunmaktadır. Bu fonksiyonlar arasında GMSK, modülasyon/demodülasyon ve kanal kodlama ve çözümü bulunmaktadır. Mobil cihaz sadece baz istasyonu ile iletişim halinde değildir, mobil yönetim (MM) ve çağrı kontrolü modülleri aracılığıyla MSC ve VLR ile de

konuşmaktadır. GSM standartları mobil cihaz için hangi özelliklerin zorunlu hangilerinin ise opsiyonel olduğunu belirtmektedir (Heine 1998). En önemli ve zorunlu olan özellikler ise;

- DTMF kabiliyeti,
- SMS kabiliyeti,
- A5/1 ve A5/2 şifreleme algoritma kabiliyeti,
- Kısa mesaj, aranan numara ve servis alınan ağ bilgilerini gösterme kabiliyeti,
- SIM olmasa bile acil çağrı yapabilme kabiliyeti,
- Gömülü IMEI numarası kabiliyetidir.

GSM protokolünün analizi ve testi için mühendislik modu aktif, test mobil cihazlara ihtiyaç duyulmaktadır. Bu cihazlar yardımıyla normalde görülmesine ihtiyaç duyulmayan GSM ağ değerlerine erişilebilmekte, söz konusu ağ değerleri manipüle edilip mobil cihazın tepkileri ölçülebilmektedir. Ayrıca baz istasyonlarının kapsama alanlarının test edilmesinde ve sıradışı GSM ağ hareketlerinin tespit edilmesinde de kullanılabilmektedir.

1.3.1.2 Baz istasyonu alt sistemleri

Hava arayüzü (um-interface, air-interface) kullanılarak Baz istasyonu alt sistemleri mobil terminal alt sistemleri ile haberleşmektedir. Baz istasyonu alt sistemleri 3 ana öğeden oluşmaktadır (Heine 1998).

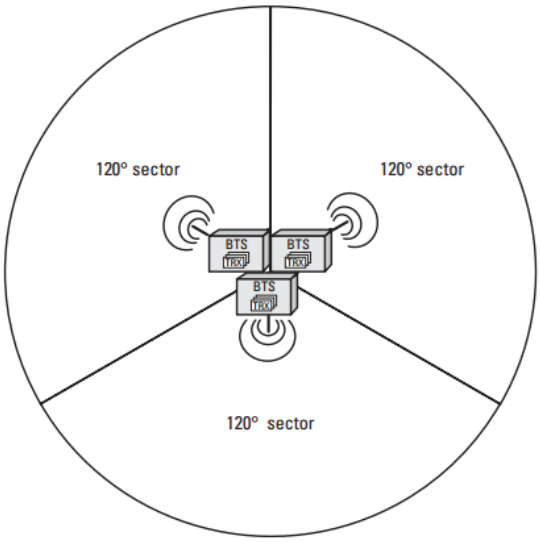
Baz İstasyonu (BTS): BTS, MT ile hava arayüzünü kullanarak fiziksel bir bağlantı kurmaktadır. Ek olarak baz istasyonları abis arayüzünü kullanarak baz istasyonu kontrolörleri (BSC) ile de bağlantı kurmaktadır.

Çizelge 1.1 SIM'de depolanan veriler (Heine, 1998'den değiştirilerek alınmıştır)

Parametre	Açıklama	Durum
Yönetimsel Veriler		
-PIN/PIN2 -PUK/PUK2 -SIM Servis Tablosu -Son Aranan Numara -Dil	-Kişisel doğrulama numarası. -PIN bloke kaldırma numarası. -SIM opsiyonel fonksiyon listesi. -Son Aranan Numara. -Geçerli dil listesi.	-Zorunlu/Değiştirilebilir. -Zorunlu/Sabit. -Zorunlu/Sabit. -Opsiyonel/ Değiştirilebilir. -Zorunlu/Değiştirilebilir.
Güvenlik Verileri		
-A3/A8 Algoritmaları -Ki Anahtarı -Kc Anahtarı -CKSN	-Doğrulama ve Kc belirleme. -SIM ve HLR tarafından bilinen numara. -A8 algoritması ile üretilen numara. -Şifreleme sıra numarası.	-Zorunlu/Sabit. -Zorunlu/Sabit. -Zorunlu/Değiştirilebilir. -Zorunlu/Değiştirilebilir.
Abone Verileri		
-IMSI -MSISDN -Erişim Kontrol Sınıfı	-Tekil abone numarası. -Abone telefon numarası. -Ağ kontrolü için kullanılır.	-Zorunlu/Sabit. -Opsiyonel/Sabit -Zorunlu/Sabit.
Dolaşım Verileri		
-TMSI -T3212 -Lokasyon güncelleme durumu -LAI -Engellenen NCC için ağ renk kodları -Tercih edilen NCC bilgileri	-Geçici tekil abone numarası. -Lokasyon güncellenmesi için. -Lokasyon güncelleme gerekli mi. -Lokasyon alanı bilgisi. -En fazla 4 engellenen PLMN bilgisi -MT'nin seçebileceği PLMN listesi	-Zorunlu/Değiştirilebilir. -Zorunlu/Değiştirilebilir. -Zorunlu/Değiştirilebilir. -Zorunlu/Değiştirilebilir. -Zorunlu/Değiştirilebilir. -Opsiyonel/ Değiştirilebilir.
PLMN Verileri		
-PLMN'nin NCC, MCC, MNC bilgileri -GSM'in ARFCN bilgileri	- NCC, MCC, MNC gibi GSM ağ bilgileri. -PLMN'nin lisanslı frekans bilgileri	-Zorunlu/Sabit. -Zorunlu/Sabit.

BTS dört ana modülden oluşmaktadır. Bunlar; alıcı/verici modülü şifreleme, şifre çözme, kodlama ve kodlamayı çözme görevlerine sahiptir. Alıcı/verici modülünde alıcı ve vericinin kendisine ait frekans hoplama (frequency hopping) unitesi vardır. İkinci modül ise operasyon ve idame modülüdür. Bu modül BSC ile bağlantı kuran ve BSC'den gelen komutları işleyen modüldür. Ayrıca sistem ve operasyon yazılımı bu modülde bulunur ve lokal yönetim için arayüz barındırır. Üçüncü modül ise "Saat (clock)"tir. Saat, genelde BSC'den alınmaktadır ama test yaparken bağımsız bir saat modülüne ihtiyaç duyulmaktadır. Baz istasyonunda bulunan bütün alıcı/vericilerin aynı saat sinyaline sahip olmaları gerekmektedir. Dördüncü modül ise girdi/çıktı filtresidir. Girdi/Çıktı filtresi gelen ve giden sinyallerin bant genişliğini kısıtlamak için kullanılmaktadır. Operasyon ve idame modülü bu filtrenin kontrolünü sağlamaktadır.

Baz istasyonlarının yerleşim/sinyal konfigürasyonları performans açısından belirleyici olmaktadır. Standart, şemsiye ve eş-konumlu (colocated) gibi baz istasyonu konfigürasyonları mevcuttur ancak genelde eş-konumlu konfigürasyon kullanılmaktadır. Eş-konumlu konfigürasyon da birden çok baz istasyonu beraber kullanılmakta ve şekil 1.4'de görüldüğü gibi kullanım yoğunluğuna göre biribirinden 30, 60, 90, 120 ve 180 derece açılarla ayrılmaktadır. Bu şekilde aynı frekans bandı bir çok baz istasyonunda kullanılabilmekte ve daha çok aboneye hizmet verilebilinmektedir.



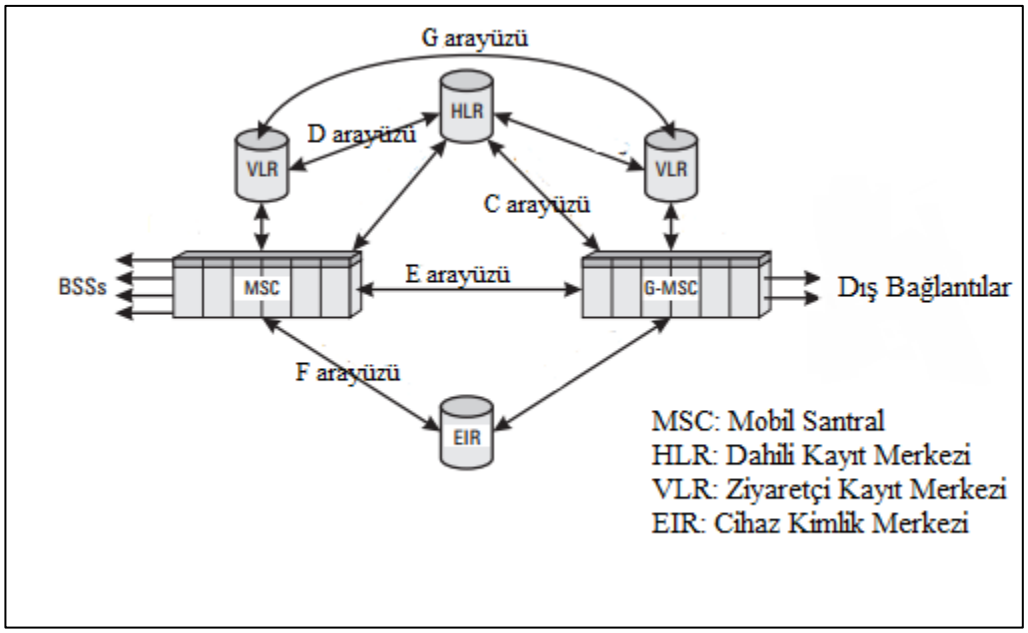
Şekil 1.4 Eş-Konumlu baz istasyonu konfigürasyonu (Heine 1998)

Baz İstasyonu Kontrolörü (BSC): Baz istasyonu alt sistemlerinin merkezinde BSC yer almaktadır. Baz istasyonları ile Abis arayüzü aracılığıyla iletişime geçmektedir. BSC, MSC (Mobile Switching Center-Mobil Santral)'den radyo ile alakalı işlerin ayrılması için kullanılmaktadır. BSC'de her bir baz istasyonu ile haberleşmeyi sağlayan Abis-TCE (terminal kontrol elementi) bulunmaktadır. Üreticiden üreticiye değişmekle birlikte, Abis-TCE'ler baz istasyonlarını kontrol etmekten de sorumludurlar. BSC ve MSC arasında ki iletişim ise A-TCE arayüzünden gerçekleşmektedir. BSC'ler bulundukları alt sistemin merkezi olduklarından, tüm alt sistemin bilgilerini içeren nispeten büyük bir veritabanı bulundurmaktadır. Söz konusu veritabanında radyo kaynaklarının kalitesi, baz istasyonları operasyonları ve dinamik olarak yönetilen işlere ait veriler bulunmaktadır. Çağrının baz istasyonları arasında el değiştirmesi ve Operasyon Merkezi alt sistemleri ile haberleşilmesi de BSC'nin görevleri arasındadır.

TRAU: TRAU BSC ve MSC arasında yer alan sıkıştırma birimidir. TRAU'nun görevi GSM üzerinden taşınan sesi sıkıştırmak ve açmaktır. 64 Kbps olan sesi 16 Kbps veya 8 Kbps'ye düşürmektedir. TRAU, doğrudan veri iletmemekte ancak iletilen veriyi sıkıştırmaktadır.

1.3.3 Ağ alt sistemleri

Ağ alt sistemleri bütün mobil ağlarda merkezi rol oynamaktadır. MT için baz istasyonu alt sistemleri radyo erişimi sağlamakta, Ağ alt sistemleri ise çağrı kurulumundan, veritabanı ve santral işlemlerine; kriptolamadan, kimlik doğrulama ve dolaşım işlemlerine kadar birçok görevi üstlenmektedir. Ağ ve operasyon merkezi alt sistemlerinin yapısı ve bunlar arasındaki iletişim şekil 1.5'de gösterilmektedir. Ağ alt sistemlerinde esnek bir topoloji vardır. Örneğin birden çok MSC bir tane EIR ile kullanılabilmekte aynı zamanda abone sayısına göre HLR sayısı artırılıp azaltılabilinmektedir (Heine 1998).



Şekil 1.5 Ağ ve operasyon merkezi alt sistemleri (Heine, 1998'den değiştirilerek alınmıştır)

Dahili kayıt merkezi (HLR): (Home Location Register). Her GSM ağında verilerin kalıcı olarak depolanması için bir tane HLR bulunmak zorundadır. Böyle bir veritabanı milyonlarca aboneye ait bilgileri tutmak zorundadır. HLR'daki veritabanının sorgulara hızlı cevap vermesi çağrı kurulum süresi için belirleyici faktörlerdendir.

HLR içinde aboneye özel bilgiler tutulmaktadır. Örneğin, çağrı güvenliği ile alakalı olan Ki verisi yalnızca burada ve SIM'de tutulmaktadır ve abonenin bilgi güvenliği için yayınlanmamaktadır. Her abonenin bilgilerinin tutulduğu HLR önceden belirlenmiştir ve kullanıcının son lokasyonu gibi bilgiler de burada tutulmaktadır.

Ziyaretçi kayıt merkezi (VLR): (Visitor Location Register). VLR, HLR benzeri bir veritabanı olmasına rağmen, farklı bir işlev görmektedir. HLR aksine, VLR daha çok dinamik verilerin yönetiminden sorumludur. Mesela MT'nin dolaşımda olduğu durumlarda, veriler eski VLR'dan yeni VLR'a aktarılmaktadır. Yeni VLR ihtiyaç halinde HLR'dan ekstra bilgiler de sorgulayabilmektedir.

MT'nin dolaşımda olmadığı (roaming) durumlarda bile dinamik verileri HLR yerine VLR tutmaktadır. Bu nedenle bir GSM ağı için tek bir HLR bulunmaktadır ancak her

bir MSC için bir tane VLR bulunmaktadır. Yani bir coğrafi alan için bir MSC ve bir VLR bulunmakta olup HLR için ise böyle bir ayrımdan söz edilemez. Çizelge 1.2'de HLR ve VLR' da tutulan veriler listelenmiştir.

Mobil Santral (MSC): (Mobile Switching Center). Teknik olarak MSC normal ISDN telefon santrallarının mobil uygulamaları destekleyecek şekilde özelleştirilmiş halidir. Kullanıcıya kanal tahsis edilmesi, MSC'ler arasında aktarımın sağlanması bu modifikasyonlardan bazılarıdır. Diğer ağlarla iletişim kuran MSC'ye G-MSC (Gateway MSC) denmektedir. Bir GSM ağında MSC'lerin yalnızca bir kısmı G-MSC olarak kullanılmaktadır. G-MSC özelliği olmayan bir MSC dış ağlara giden çağrıları G-MSC'lere yönlendirmek zorundadır. MSC ve VLR ayrı ayrı yerleştirilebiliyor olmasına rağmen GSM ağ operatörleri kullanım kolaylığı açısından iki üniteyi beraber kullanmayı tercih etmektedirler.

1.3.1.4 Operasyon merkezi alt sistemleri

Operasyon merkezi alt sistemi, kimliklerin doğrulanmasını baz alan sistem güvenliğinden sorumludur. Bu alt sistemde iki öğe bulunmaktadır (Heine 1998).

Doğrulama Merkezi (AuC): (Authentication Center). AuC, HLR'ın bir parçası olarak geliştirilmiştir. AuC nin tek önemli görevi, kimlik doğrulama işlemi esnasında, kullanıcının kimlik doğrulaması sırasında kullandığı üçlü değeri (SRES, RAND, Kc) üretip HLR'a göndermesidir. Sonrasında HLR bu üçlüleri VLR'a göndermekte ve VLR bunları kimlik doğrulama ve şifreleme için kullanmaktadır.

Cihaz Kimlik Merkezi (EIR): (Equipment Identiy Register). GSM mimarisinde mobil cihaz ile SIM'in ayrılması, geçerli bir SIM'in yasaklı bir mobil cihaz ile kullanılması tehlikesini gündeme getirmiştir. EIR de bu cihazların belirlenip, takip edilmesi için kullanılmaktadır. Bölüm 1.3.1.1'de bahsedildiği gibi her mobil cihazın tekil bir IMEI numarası bulunmalıdır. Ülkemizde MCKS (Mobil Cihaz Kontrol Sistemi) bu verileri kullanmaktadır.

Çizelge 1.2 HLR ve VLR'da tutulan önemli veriler (Heine 1998'den değiştirilerek alınmıştır)

Parametre	HLR/AuC	VLR
Abone Bilgileri		
-IMSI	+	+
-Ki	+	
-TMSI		+
-Servis Kısıtlaması	+	
-Ek servisler	+	+
-MSISDN(basit)	+	
-MSISDN(diğer)	+	
Kimlik Doğrulama ve Şifreleme		
-A3	+	
-A5/X		
-A8	+	
-RAND	+	+
-SRES	+	+
-Kc	+	+
-CKSN		+
Abone Lokasyonu/Çağrı Yönlendirme		
-HLR numarası		+
-VLR numarası	+	
-MSC numarası	+	+
-LAI		+
-IMSI ayırma		+
-MSRN		+
-LMSI	+	+
-Devir (Handover)		+

HLR ve VLR'de olduğu gibi EIR'de bir veritabanı işlevi görmektedir. EIR'de üç çeşit veri tutulup bu verilerin güncelliği sağlanmaktadır. Bunlar aşağıda sıralanmıştır (Anonymous 1992) .

- Beyaz Liste: Onaylanmış mobil cihaz IMEI listesi
- Kara Liste: Çalıntı veya yasaklanmış mobil cihaz IMEI listesi
- Gri Liste: Bir nedenle takip edilen MT'lerin listesi.

1.3.2 GSM arayüzleri

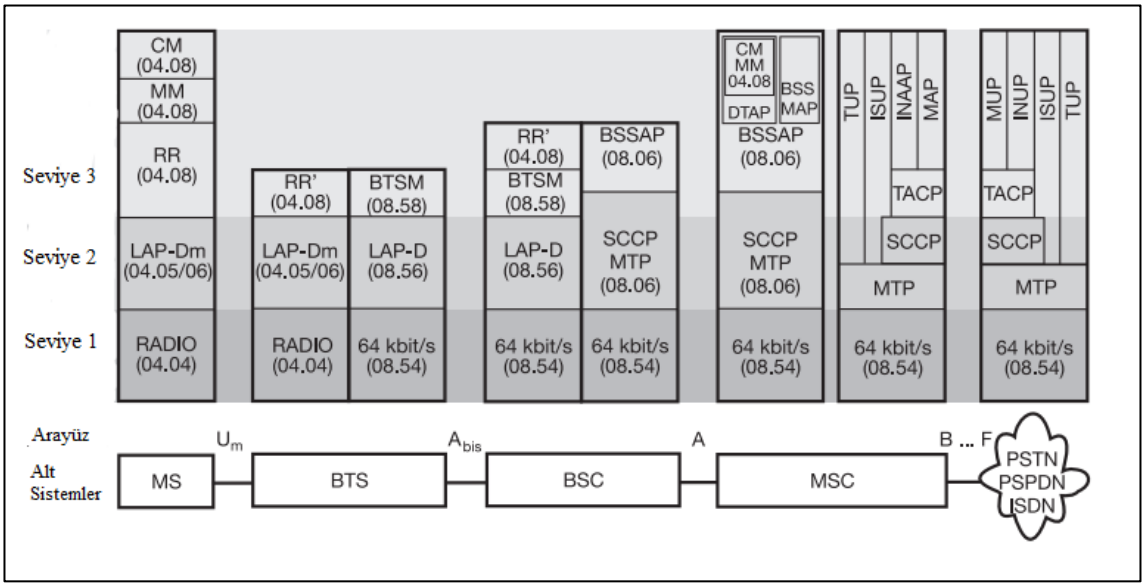
GSM protokollerinde referans olarak OSI modeli kullanılmış olup, OSI modelindeki 3 ana katman kullanılmıştır (Heine 1998). Bu katmanlar ve genel görevleri ve özellikleri aşağıda sunulmuştur. Bu kısım özet halinde verilecektir.

1. Katman 1: Fiziksel katman (Physical layer)
    a. Fiziki iletim (TDMA, FDMA...),
    b. Kanal kalitesinin değerlendirilmesi,
    c. Hava arayüzü haricinde PCM 30 veya ISDN bağlantıları kullanılmaktadır.
2. Katman 2: Veri hattı katmanı (Data link layer)
    a. Katman 2 bağlantıların çoklanması ve kontrol ve sinyal kanallarının yürütülmesi,
    b. Hata tespiti (Error detection),
    c. Akış kontrolü (Flow control),
    d. İletim kalite güvencesi,
    e. İletim (Routing).
3. Katman 3: Ağ katmanı
    a. Hava arayüzü için bağlantı yönetimi (Connection management),
    b. Lokasyon bilgisi yönetimi,
    c. Abone belirlenmesi,
    d. SMS, çağrı yönlendirme gibi ek servislerin yönetimi.

GSM ağında verinin alt sistemler arasında geçişi için çeşitli protokoller gerekmektedir. Şekil 1.6 alt sistemleri birbirine bağlayan arayüzleri ve bunların barındırdığı fonksiyonların katmanlara göre dağılımını göstermektedir.

1.3.2.1 Abis arayüzü

Baz istasyonu ve BSC arasındaki PCM 30 arayüzüdür. GSM spesifikasyonlarında detaylı olarak bahsedilmemiştir. Bu nedenle üreticiler arasında 2. Katmanda varyasyonlara sebep olmuştur. Baz istasyonları ile BSC'ler arasındaki bağlantı şekilleri için farklı ağ konfigürasyon alternatifleri mevcuttur. Örnek olarak seri, yıldız bağlantı modelleri söz konusu konfigürasyonlar için kullanılabilmektedir (Kahabka 2014) .



Şekil 1.6 GSM katmanları ve arayüzleri (Kahabka 2014'den değiştirilerek alınmıştır)

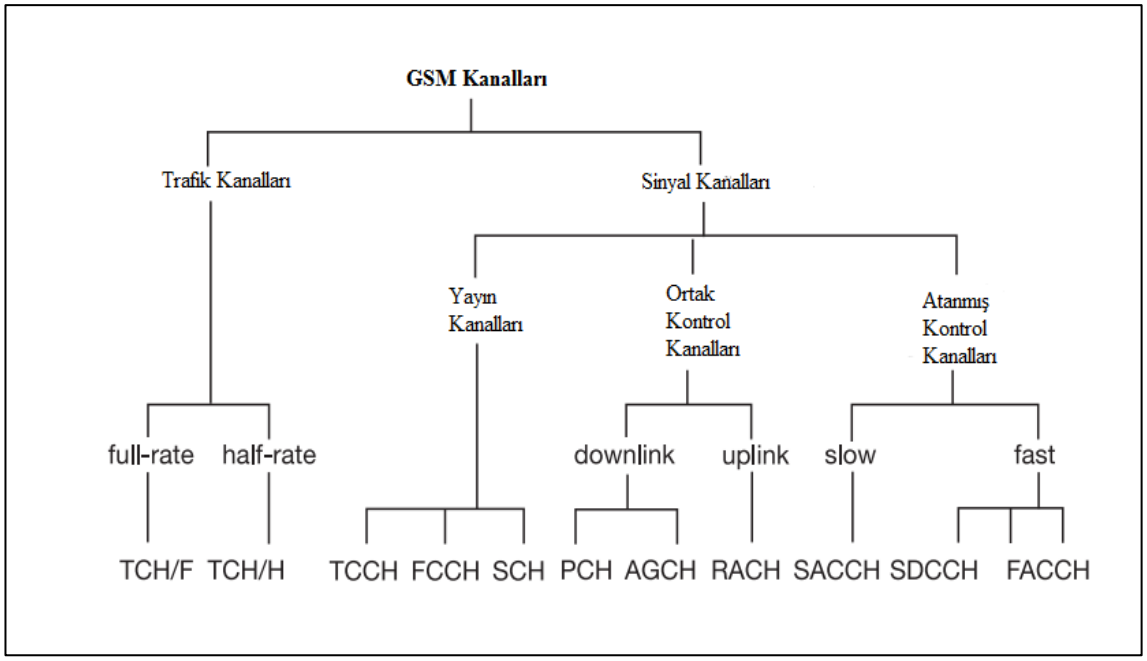
1.3.2.2 Hava-Um arayüzü

Hava arayüzü bütün mobil ağların merkezi konumunda olup kullanıcı ile iletişimi olan tek arayüzdür. Hava arayüzünün fiziksel karakteri de mobil standartın başarısı ve kalitesi için de önemli olmaktadır. Sınırlı frekans kaynağının etkin kullanılması hava

arayüzü ile gerçekleşmekte ve söz konusu frekans kaynağının etkin kullanılması gerekmektedir.

GSM hava arayüzünde FDMA (Frequency division multiple access) ve TDMA'in (Time division multiple access) kombinasyonunu kullanmaktadır. FDMA kullanan bir sistemde sinyal kalıcı olarak gönderilmekte ancak TDMA'de her kullanıcı kendisini ayrılan zaman periyodunda sinyaller göndermektedir. Bu da TMDA'e aynı frekansda 7 ayrı kanala hizmet verme imkânı tanımakta ve TDMA'in FDMA'e olan üstünlüğünü ortaya koymaktadır (Kahabka 2014) .

Bir takım mantıksal kanallar fiziksel kanallara eşlenmiştir. Söz konusu kanallar yukarı yönlü (uplink) ve/ya aşağı yönlü de (downlink) olabilmektedir. Mantıksal bir kanal kullanıcı verisini taşıyan trafik kanalı veya sinyalizasyon kanalı olabilmektedir. Söz konusu kanallara ait şema şekil 1.7'de sunulmaktadır.



Şekil 1.7 GSM kanalları (Kahabka 2014'den değiştirilerek alınmıştır)

Trafik kanalları: (TCH) konuşma ve veri trafiğini taşımaktadır. TCH 26 TDMA grubu kullanacak şekilde tanımlanmıştır. Tam-oranlı (full-rate, 22 kbit/s) ve yarı-oranlı

(half-rate 11.4 kbit/s) trafik kanalları da tanımlanmıştır. Yarı-oranlı kanalları kullanarak bir kanal üzerinden iki görüşme yaptırmak mümkün olmaktadır.

Hava arayüzündeki sinyalizasyon kanalları çağrı kurulumu, radyoyla arama (paging), çağrı idamesi ve senkronizasyon gibi işlerde kullanılmaktadır. 3 grup sinyalizasyon kanalı vardır.

Yayın kanalları (BCH): (Broadcast channels): Sadece aşağı yönlü bilgi taşır. Genel anlamda senkronizasyon ve frekans düzeltme işlemlerinden sorumludur. **Tez içeriğinde bu kanaldan aktarılan veriler yoğun olarak kullanılmaktadır.** BCH içinde 3 kanal daha vardır.

Yayın kontrol kanalı (BCCH): (Broadcast control channel), genel bilgileri, hücre bilgilerini, lokasyon alanı bilgilerini (LAI- Location Area Identifier), Ağ operatör bilgilerini, Ağ erişim bilgilerini, komşu hücre bilgileri gibi bilgileri yayınlar. Tez'de takip ettiğimiz kanaldır. Mobil cihaz kendi GSM operatörünün veya diğer operatörlerin BCCH kanalından bilgiler alır.

Frekans düzeltme kanalı (FCCH) (Frequency correction channel), MT'nin frekans düzeltmesi, frekans standardının MT'ye iletilmesi için kullanılır. TDMA'in ilk zaman aralığının senkronizasyonu için de kullanılır.

Senkronizasyon kanalı (SCH) (Synchronization channel) TDMA frame numarasının senkronizasyonu ve baz istasyonunun belirlenmesi için kullanılır. SCH kanalından gelen bir veri demeti (burst) MT'nin BTS ile senkronize olması için yeterlidir.

Ortak Kontrol Kanalları (CCCH): (Common control channels), aşağı yönlü ve yukarı yönlü kanallardır. GSM ağından mobil cihaza bilgi iletilmesi içindir. Alt kanalları vardır.

- Paging kanalı (PCH),: Mobil cihaza çağrı geldiğini haber veren kanaldır.

- Erişim kanalı (AGCH): Baz istasyonun MT için ayırdığı TCH kanalı bilgisini MT'ye gönderen kanaldır.
- Rastgele erişim kanalı (RACH): Sadece yukarı yönlüdür. Mobil cihazın, baz istasyonundan SDCCH kanalı talebini içerir.

Atanmış Kontrol Kanalları (DCCH): (Dedicated control channels) dolaşımdan, şifrelemeden, çağrı geçişlerinden sorumludur. Alt kanalları vardır.

- Ayrık atanmış kontrol kanalı (SDCCH): (Stand-alone dedicated control channel), MT ve BTS arasındaki çağrı kurulumu sırasında TCH atanmadan önceki kanaldır.
- Yavaş ilişkili kontrol kanalı (SACCH): (Slow associated control channel) TCH ve SDCCH için ölçüm raporlarını gönderir.
- Hızlı ilişkili kontrol kanalı (FACCH): (Fast associated control channel) SACCH'ın veri aktarım hızı yeterli olmadığında SACCH ile benzer durumlar için kullanılır.

1.3.2.3 A arayüzü

A arayüzü BSC ve MSC arasındadır. Bir veya daha çok PCM hatları içerir. Her bir hattın 2 Mbps bant genişliği vardır. Bu arayüzün iki parçası vardır. Birinci parça BSC ve TRAU arasındadır. İkinci parça ise TRAU ile MSC arasındadır. Sıkıştırma işlemi TRAU'da yapıldığından, veri TRAU ve MSC arasında bulunan ikinci parçadan itibaren sıkıştırılmış olarak taşınmaktadır.

2. KAYNAK ÖZETLERİ

Yapılan literatür araştırmaları sonucunda sahte baz istasyonu saldırılarının tespit edilmesine yönelik çalışmaya rastlanılmamış olup, İnternet ortamında başlangıç aşamasında bazı çalışmalara rastlanmıştır. Bununla birlikte, sahte BTS saldırılarının geliştirilmesi ile alakalı literatür araştırmalarında az sayıda çalışma bulunmuştur. Söz konusu çalışmalardaki saldırı yaklaşımları, saldırıların tespitine yönelik algoritma geliştirmek için kullanılmış ve detayları aşağıda özetlenmiştir.

Vales-Alonso vd. (2001) yaptığı çalışmada, konferans salonları veya uçaklar gibi MT'lerin aktif olmaması gereken alanlarda, MT'lerin tespit edilip yasaklanması için bir sistem geliştirilmiştir. Çalışma kapsamında GSM protokolünün ilgili kısımları analiz edilmiş olup, çalışmaya göre, MT'ler birkaç durumda kendini şebekeye tanıtmaktadırlar, yani kendilerine özgü olan IMSI numaralarını şebekeye bildirmektedirler. Bu çalışmada yazarlar bu durumların 3'ünden bahsetmişlerdir: 1) Gelen/giden aramalarla; 2) Zamanlayıcıların (T3211, T3213 ve T3212) süresinin dolmasıyla; 3) Yeni bir bölgeye (Location Area) girilmesiyle. Birinci durum için, MT'nin kendini şebekeye tanıtması RF alıcılar ile tespit edilebilmekte ancak uygulanabilir olmamaktadır. İkinci durumda MT'nin kendini şebekeye tanıtmasının yakalanması zordur çünkü söz konusu zamanlayıcıların süresi her GSM operatöründe değişiklik göstermekte ve bu süreler genellikle saat mertebesinde olmaktadır. Çalışmanın hedefi üçüncü durumla ilgili olup, bu durumun iki adımı vardır. İlk adım, sinyal bozucu (jammer) yardımıyla hedef alandaki bütün aktif BTS'leri devre dışı bırakmaktır (Pousada-Carballo vd. 1998). İkinci adım ise, farklı bir LAI değerine sahip sahte BTS kullanmaktır. Çalışmaya göre, MT ile gerçek BTS'lerin bağlantısı kesildiğinde, MT otomatik olarak yeni BTS'ler arayacaktır. MT'nin bulabileceği tek BTS ise sahte BTS olacaktır. Sonrasında, MT sahte BTS'e bağlanacak ve BTS'in LAI değerinden farklı bir bölgeye ait olduğunu değerlendirecektir. Farklı bölgedeki BTS'e bağlanılması lokasyon güncelleme sürecini tetikleyecek ve MT'nin IMSI numarasını ileterek kendini sahte BTS'e tanıtmasına sebep olacaktır. Çalışmada kısmi başarı elde edilmiş olup bu alanda ilerlemeler olabileceği gösterilmiştir. Bu bilgiler ışığında, sahte

BTS saldırılarının anlaşılması için beklenmedik LAI değişikliklerinin takip edilmesi gerektiği anlaşılmaktadır.

González-Castaño vd. (2003) yaptıkları çalışmada, GSM protokolünü hedef alan gerçek zamanlı detektör sistemi geliştirilmiştir. Vales-Alonso vd. (2001) yaptığı çalışmada olduğu gibi bu çalışmada da ilgili GSM protokolü analiz edilmiş ve önceki çalışmaya ek olarak MT'nin kendini ağa tanıtması için 2 yöntem daha kullanılmıştır. Bunlar ise, MT'lerin açılışta ve çağrı düşüp tekrar bağlanmak istediğinde yaptığı lokasyon güncelleme istekleridir. Geliştirilen detektör sistemi üç parçadan oluşmaktadır. Birinci parça, önceki çalışmada geliştirilen "GSM MT detektörü" (Vales-Alonso vd. 2001) ikincisi lokal veri tabanı, üçüncüsü ise seçici yakalama (selective interceptor) cihazıdır. Çalışmayla, belirli bir bölge içinde kalan MT'ler "GSM MT Detektörü" ile tespit edilmekte ve tespit edilen MT kimlikleri lokal veri tabanında toplanmaktadır. Sonrasında ise, MT'ler lokal veri tabanından kontrol edilerek seçici olarak engellenip bırakılabilmektedir. Bu çalışma ile kavram kanıtlama (proof of concept) olan ilk çalışma daha etkin kullanılmış olup, söz konusu çalışma ürünleştirilmeye çalışılmıştır. Yapılan çalışmalarda hedef MT'lerin sadece bir kısmı saldırının etkisine girmiş olup, saldırının etki etme süresi gerçek ortamda kullanılamayacak kadar uzun olduğu değerlendirilmektedir.

Zhou vd. (2010) ve Song vd. (2012) yaptıkları çalışmalarda, yazılımsal radyo teknolojisi (software radio technologies - SDR) kullanılarak sahte BTS geliştirilmiştir. Bu çalışmada önceki iki çalışmanın aksine sahte BTS geliştirilirken, gerçek BTS'ler sinyal bozucu ile engellenmemiştir (González-Castaño vd. 2003), (Vales-Alonso vd. 2001). Ayrıca, sahte BTS geliştirilirken farklı bir yaklaşım ve yazılımsal radyo teknolojisi kullanılması hem masrafları düşürmüş hem de performansı önemli oranda artırmıştır. Yapılan çalışmalarda GSM protokolü detaylı olarak incelenmiş, protokolün açıkları geliştirilen yazılım ve donanımlarla manipüle edilerek son kullanıcıya hitap edebilecek performansta bir ürün ortaya konulmuştur.

Geliştirilen sistemde bir tane mühendislik maduna sahip MT kullanılmıştır. Söz konusu MT ile çevredeki aktif BTS'ler tespit edilebilmektedir. Tespit edilen BTS'ler hücre

seçilme kriteri olan C2 parametresine göre (cell reselection criterion) güçlüden zayıfa sıralanmaktadır. Sahte BTS, bahse konu MT'den BTS'lere ait bilgileri alıp, ortamdaki en zayıf BTS gibi davranmakta ve hedef MT'lerin kendisine bağlanmasını sağlamaktadır. Gerçek BTS'in taklit edilmesinin sebebi, normal BTS'lerin komşu BTS'lere ait bilgileri olası bir devir durumunda, MT'yi yönlendirmek amaçlı, BCH'dan yayınlamalarıdır. Böylece MT'ler tereddüt etmeden sahte BTS'e bağlanmaktadır. Sahte BTS, taklit ettiği BTS'in MCC (Mobile Country Code) ve MNC (Mobile Network Code) gibi GSM operatörlerine ait olan bilgilerini de taklit etmelidir. Bu nedenle, amaç ortamdaki tüm MT'ler ise her GSM operatörü için ayrı sahte BTS kullanılmalıdır. Bununla birlikte, MT'nin kendini sahte BTS'e tanıtması için MT'lerde lokasyon güncelleme prosedürü tetiklenmelidir. Söz konusu tetiklenme için sahte BTS'in LAI değeri gerçek BTS'lerden farklı olmalıdır. Çalışmadaki en kritik bölüm, sahte BTS'in yayın yapan en güçlü BTS olmasa bile kendini MT'lere seçtirebilmesidir. MT'ler, her 5 saniyede BTS'lerin BCCH'ını okuyup, C2 parametresine göre BTS'leri güçlüden zayıfa dizmektedir. MT için BTS seçimi BTS'lerin C2 parametrelerine göre yapılmaktadır. C2 parametresi MT'nin BTS'e yakınlığı ve bazı ofset değerleri ile hesaplanmaktadır. Ofset değerlerine pozitif/negatif değerler verilerek MT'nin spesifik bir BTS'i seçimi teşvik edilebilmekte veya engellenebilmektedir. Çalışmada, geliştirilen sahte BTS, C2 parametresini değiştirerek MT'lerin kısa sürede kendisine bağlanmalarını sağlayabilmiştir. Ayrıca, farklı LAI kullanılarak MT'lerde lokasyon güncelleme prosedürü tetiklenebilmiştir. Sonuç olarak, sahte BTS saldırılarının tespit edilebilmesi için sıra dışı C2 değerleri önemli bir gösterge olacağı, ayrıca zayıf olan BTS'in beklenmedik şekilde seçilmesine de dikkat edilmesi gerektiği anlaşılmıştır.

Borgaonkar vd. (2014), Amerika Birleşik Devletlerinde düzenlenen "BlackHat" konferansında "IMSI Güvenliğini Anlama (Understanding IMSI Privacy)" adı altında sahte BTS saldırılarının tespitine yönelik bir çalışma yapmışlardır. Söz konusu çalışmada sahte BTS saldırıları sırasında, saldırganın, MT'nin yerini tespit için kullanıcı tarafından görülmeyen sessiz SMS gönderdiği ifade edilmiş olup, söz konusu SMS'in ANDROID işletim sistemine sahip akıllı telefonla tespit edilip kullanıcıyı uyardığı aktarılmıştır. Fakat bahse konu sessiz SMS yönteminin legal takip amacıyla

kullanılabileceğinden, verilen uyarının sahte BTS saldırısı olmayabileceği değerlendirilmektedir.

Hâlihazırda internet üzerinden sahte BTS saldırısı yapan cihaz "IMSI Catcher" adı altında satılmaktadır. Septier firmasının web sayfasında el tipi ve standart cihazlar satışa sunulmaktadır. Söz konusu cihazların spesifikasyonları incelendiğinde, cihazların 3G ağında çalışamadığı için cihazın bulunduğu ortamdaki 3G BTS'leri sinyal bozucu ile bastırıp MT'leri 2G kullanmaya zorladığı, sonrasında da mevcut saldırı cihazı kullanılarak ortamdaki MT'lere ait IMSI numaralarının toplanabildiği öğrenilmiştir. 3G ağında 2G'de bulunan karşılıklı doğrulama eksikliği olmadığından bu cihazların 3G'de çalışmaması beklenen bir durum olup ortamdaki 3G BTS'lerin sinyal bozucu kullanılarak bastırılmış olması sahte BTS saldırısı hususunda algoritma için belirleyici unsurlardan birisi olacaktır (Anonymous 2014e).

Sahte BTS saldırısı, BTS ve MT arasında gerçekleşen bir tür man-in-the-middle saldırısıdır. Yukarıdaki çalışmalardan anlaşıldığı üzere, sahte BTS saldırıları için MT'nin BTS'e bağlanması gerekmektedir. Bu bağlantının sağlanması için C2 parametresinin manipüle edilmesi önemli olmaktadır. Ayrıca farklı bir LAI kullanarak MT'nin kimliğinin alınması da gerekmektedir. Sahte BTS saldırı tespit algoritması yukarıdaki yaklaşımlar göz önünde bulundurularak geliştirilmiştir.

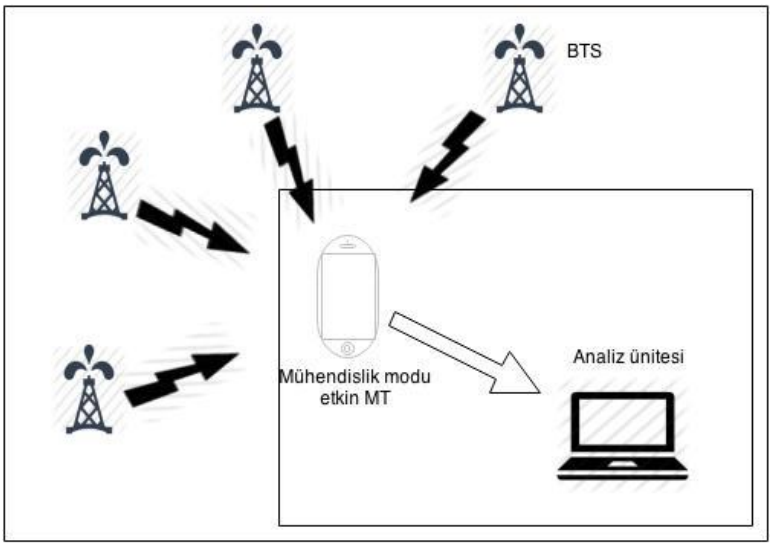
3. MATERYAL VE YÖNTEM

Önceki bölümlerde bahsedildiği gibi literatür araştırmalarında sahte BTS saldırıları ile ilgili çalışmalar bulunmasına rağmen, bu saldırıların tespit edilmesine yönelik çalışmaya rastlanılmamıştır. Bu çalışma ile GSM protokolü incelenmiş ve sahte BTS saldırıları analiz edilmiş olup, çalışmanın sahte BTS saldırılarının tespiti alanına katkı sağlayacağı düşünülmektedir.

3.1 Sistem Mimarisi

Sahte BTS saldırılarının tespitine yönelik önerilen sistem mimarisi şekil 3.1'de sunulmaktadır. Şekildeki mühendislik modu etkin olan MT, kendi bölgesindeki aktif BTS'leri tespit edip, Cell ID, MCC, MNC, LAI gibi BTS'ler ile alakalı bilgileri almak için erişim alanındaki BTS'lerin BCCH'ını okumaktadır. Söz konusu MT, BTS'lerden topladığı bilgileri "Analiz ünitesine" yollamaktadır. Ek olarak, MT BTS'lerden okuduğu bilgileri kullanarak otomatik olarak hesapladığı C1 (cell selection parameter) ve C2 (cell reselection parameter) parametrelerini de analiz ünitesine göndermektedir. Geliştirilen algoritmayı çalıştırabilecek herhangi bir PC veya akıllı telefon analiz ünitesi olarak kullanılabilmektedir. Analiz ünitesi, MT'nin gönderdiği verileri sahte BTS saldırı tespit algoritmasına göre değerlendirip, şüpheli durumları kullanıcıya raporlamaktadır.

Mühendislik modu etkin MT ile analiz ünitesinin veri iletim şekilleri ve konumları değiştirilerek daha farklı mimariler oluşturmak mümkün olabilecektir. Bu kapsamda mevcut mimariye alternatif olarak merkezi bir analiz ünitesi kurulup, GSM bilgilerini toplayan MT'ler, internet üzerinden bilgileri merkezi analiz ünitesine gönderip, sonuçlarını alabileceği mimarilerin kullanımı da imkan dahilinde olacaktır. Ayrıca GSM bilgilerini toplayan MT ile analiz ünitesini uygun bir donanım kullanarak tek bir platformda toplayıp, sonuçları hızlı bir şekilde analiz eden mobil bir sistem kurulumu da söz konusu saldırıların tespitini oldukça kolaylaştıracaktır.



Şekil 3.1 Sistem Mimarisi.

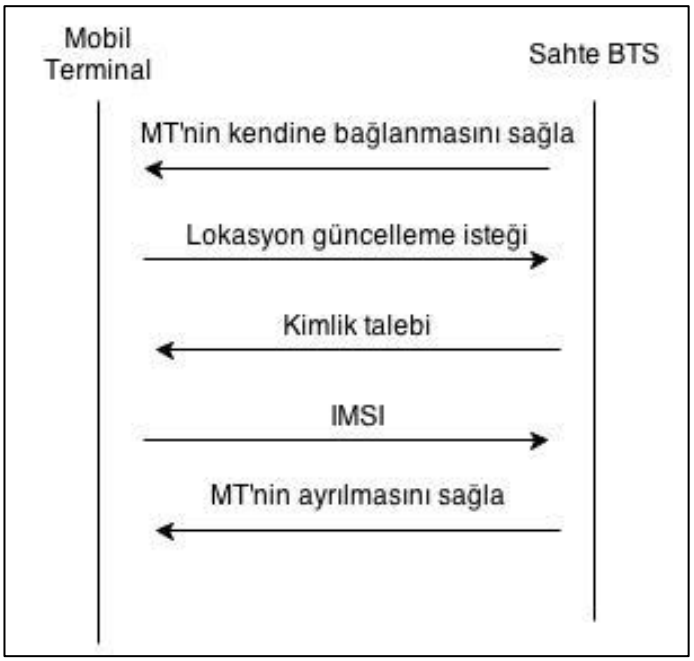
3.2 Protokol Analizi

Sahte BTS saldırıları man-in-the-middle saldırılarının tipik örneklerindendir. Söz konusu saldırı türünün çeşitli varyasyonları olmasına rağmen hepsinin ortak noktası MT'lerle BTS arasına girilmesi ve MT'lerin IMSI/IMEI numaralarının ele geçirilerek hedeflerin tanınmasıdır. Temel bir sahte BTS saldırısı şekil 3.2'deki gibi gerçekleşmektedir.

MT'lerin sahte BTS ile kimliğinin ele geçirilmesi lokasyon güncelleme sürecinin tetiklenmesi ile yapılabilmektedir (Zhou vd. 2010), (Song vd 2012). İkinci bölümde ve ilgili GSM spesifikasyonlarında açıklandığı üzere, lokasyon güncellemesinin tetiklenebilmesi için birçok yöntem bulunmaktadır. Bunlar aşağıdaki listede sunulmuştur (Anonymous 1992).

- Yeni bir lokasyon bölgesine girildiğinde
- Telefonda saklanan son kayıtlı lokasyon bölgesi kaybolduğunda
- Süresi 6 dakika ile 25,5 saat arası değişebilen zamanlayıcının süresi dolduğunda
- Çağrı başlangıç ve bitişinde

Telefonda saklanan son kayıtlı lokasyon verisine, GSM operatörü tarafından belirlenen zamanlayıcının süresine ve MT kullanıcısının çağrı başlangıç ve bitişine müdahale edilemediğinden, sahte BTS'ler kendilerini başka bir lokasyon bölgesinden göstererek lokasyon güncelleme sürecini tetikleyip kullanıcının kimlik bilgilerine ulaşabilmektedirler (Song vd. 2012).



Şekil 3.2 Örnek sahte BTS saldırısı

Şekil 3.2'de de görüldüğü gibi, Sahte BTS saldırısı yapmak için öncelikle MT ile GSM ağı arasına sahte BTS kullanarak girilmesi gerekmektedir. Sahte BTS saldırıları için, MT'nin yakalanması ve bırakılması en zor kısımdır. Önceki çalışmalarda sinyal bozucu sistemler kullanılmış ve MT' için bağlanmaya aday baz istasyonu bırakmadan MT'nin sahte BTS'i seçmesi beklenmiştir (Vales-Alonso vd. 2001), (González-Castaño vd. 2003). Fakat bu sistemlerde her BTS için ayrı bir sinyal bozucu ünite gerekmekte ve sinyal bozucunun zamanlamasını ayarlarken zorluklarla karşılaşılmaktadır. Literatürdeki son makalelerde ise C1 ve C2 parametresinin manipüle edilerek kullanılması yöntemi seçilmiş ve bu yöntem hem masrafı düşürmüş hem de performansı önemli ölçüde artırmıştır (Zhou vd 2010), (Song vd. 2012).

GSM protokolüne göre hücre seçimi (cell selection & reselection) için bazı kurallar konulmuştur. Bu kurallara göre; MT en fazla 5 saniyede bir, ortamda bulunup hizmet alınmayan 6 en güçlü BTS'in BCCH bilgilerini okumaktadır. Sonrasında hizmet veren hücrenin ve komşu hücrelerin C1 ve C2 değerlerini hesaplamaktadır (Anonymous 1998), (Anonymous 1999).

Hücrenin tekrar seçilimin (cell reselection) gerçekleşmesi için aşağıda belirtilen kriterlerin sağlanması gerekmektedir (Anonymous 1992).

- Eğer hücreler aynı lokasyon bölgesinde ise; hizmet vermeyen hücrenin C2 değeri hizmet veren hücrenin C2 değerinden 5 saniye boyunca daha büyükse,
- Eğer iki hücre farklı lokasyon bölgesinde ise; hizmet vermeyen hücrenin C2 değeri, hizmet veren hücrenin C2 değerinden 5 saniye boyunca hizmet veren hücrenin BCCH'ından yayınlanan CELL_RESELECT_HYSTERESIS dB kadar büyükse,
- Hizmet veren hücrenin C1 değeri 5 saniye boyunca sıfırın altında düştüyse,
- Hizmet veren hücre operatör tarafından yasaklandıysa,
- MT'nin downlink sinyal hatası sayacı (DSC) dolduysa hücre seçimi gerçekleşir.

Eğer sahte BTS'in C2 değeri hizmet veren hücreden en azından CELL_RESELECT_HYSTERESIS kadar fazlaysa ve sahte BTS'in LAI değeri hizmet veren hücreden farklıysa, sahte BTS MT'nin IMSI numarasını alabilmektedir. GSM protokolüne göre C1 ve C2 değerleri aşağıdaki gibi hesaplanmaktadır.

$$C1 = (A - Max(B, 0)) \tag{3.1}$$

$$A = RLA\_C - RXLEV\_ACCESS\_MIN \tag{3.2}$$

$$B = MS\_TXPWR\_MAX\_CCH - P \tag{3.3}$$

Sınıf 3 DCS 1800'ler için,

$$B = MS\_TXPWR\_MAX\_CCH + POWER\_OFFSET - P \tag{3.4}$$

Yukarıdaki formüllerde;

- RLA_C ulaşılan ortalama değerler
- RXLEV_ACCESS_MIN MT'nin sisteme erişmesi için gerekli minimum sinyal seviyesi;
- MS_TXPWR_MAX_CCH MT'nin sisteme erişmesi için gerekli olan en fazla TX güç seviyesi
- POWER_OFFSET MS_TXPWR ile karşılıklı olarak kullanılan güç ofset değeri
- P, MT'nin maksimum RF güç çıkışıdır.

Bütün değerler dBm formatındadır ve yukarıdaki tanıma göre, C1 değeri MS ve BTS arasındaki mesafe ile ters orantılıdır. C2 parametresi ise hücre seçimi için kullanılmakta ve aşağıdaki gibi tanımlanmaktadır.

PENALTY_TIME <> 11111 için,

$$C2 = C1 + CELL\_(RESELECT\_OFFSET\ ) - TEMPORARY\_OFFSET * H(PENALTY\_TIME - T) \quad (3.5)$$

PENALTY TIME = 11111 için,

$$C2\ =\ C1 -\ CELL\_RESELECT\_OFFSET \quad (3.6)$$

Komşu hücreler için,

$$H\ x\ =\ \begin{matrix} 0, x < 0 \\ 1, x \geq 0 \end{matrix} \quad (3.7)$$

Hizmet veren hücre için,

$$H\ x\ = 0 \quad (3.8)$$

T, hesaplanan en güçlü BTS'ler listesinde her BTS için tutulan zamanlayıcıdır.

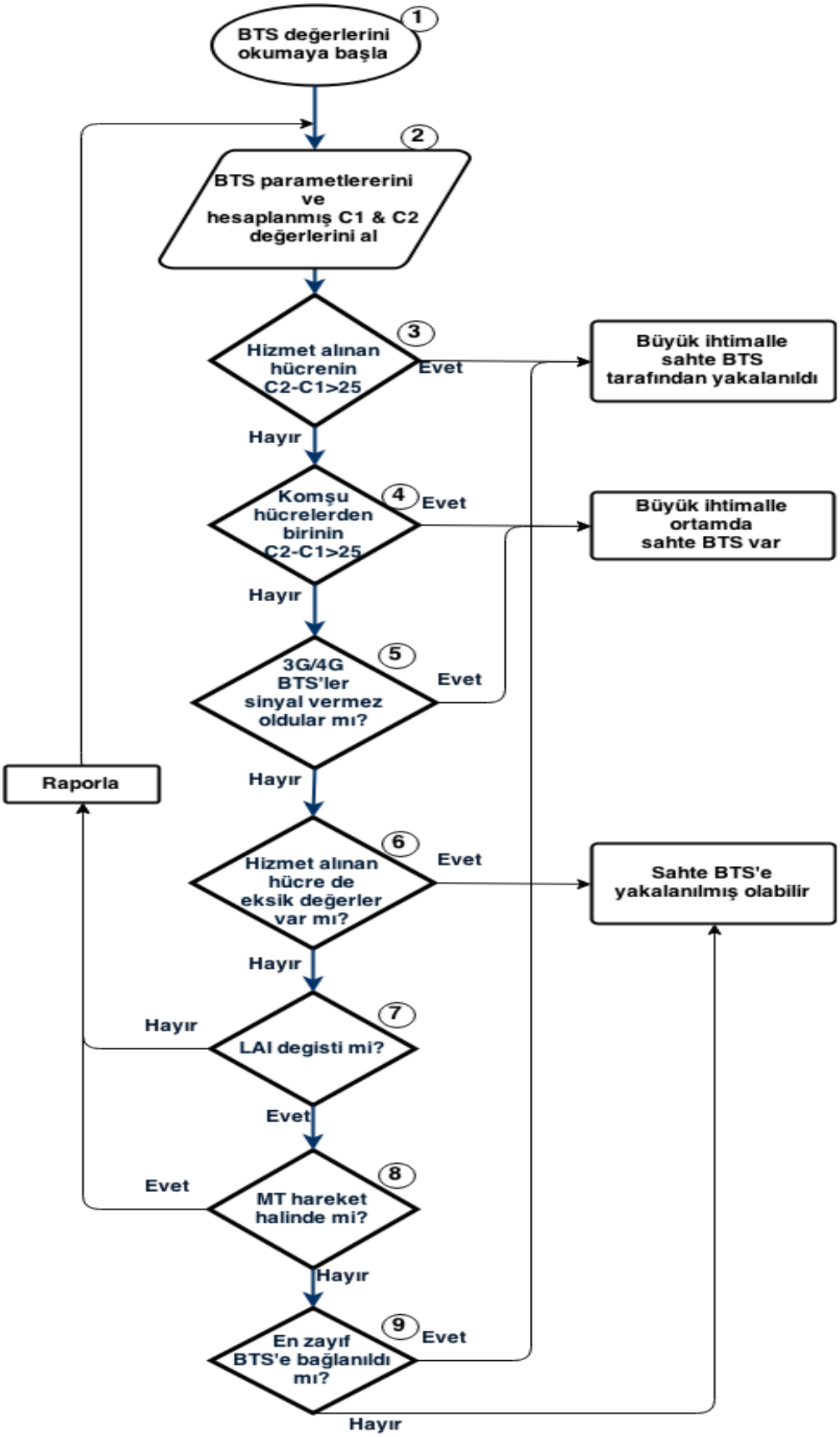
CELL_RESELECT_OFFSET, TEMPORARY_OFFSET, PENALTY_TIME, CELL_BAR_QUALIFY değerleri opsiyonel olarak BTS'in BCCH kanalından yayınlanmaktadır. Eğer yayınlanmıyorsa olağan değerleri sıfıra eşittir ve bu şekilde yaklaşık olarak C2 ve C1 birbirlerine eşit olur. Türkiye'nin Ankara ilinde yapılan testlerde, test edilen BTS'ler için GSM protokolüne de uygun şekilde, eşitlik 3.9'da belirtilen ilişki gözlemlenmiştir. Eşitlikte gözüken fark anlık olmakta ve hemen eşitlenmekle birlikte, hava arayüzü aracılığıyla yayınlanan değerlerin iletim ortamı kaynaklı bozulması olarak değerlendirilmektedir.

$$C2 - C1 \leq 4 \tag{3.9}$$

Yukarıdaki hesaplamalara ve GSM protokolünün ilgili kısımlarına göre BTS'ler arasında öncelik tanımak için söz konusu opsiyonel parametreler kullanılmaktadır. Opsiyonel parametreler C2 değerini değiştirmek için kullanılabilir ve BTS'in hesaplanmış C2 değeri ne kadar yüksek olursa MT'nin BTS'i seçme ihtimali o kadar artar. C2 değerinin olağan dışı bir şekilde C1 değerinden farklı olması şekil 3.3'de gösterilen sahte BTS tespit algoritması için önemli bir girdi olacaktır.

3.3 Algoritma Tasarımı

Şekil 3.3'de sahte BTS tespit algoritmasının akış şeması verilmektedir. Algoritma ağ değerlerini ve MT lokasyonunu değerlendirmektedir. Algoritma sıra dışı durumlarla karşılaştığında 3 tür rapor üretmektedir.



Şekil 3.3 Sahte BTS Saldırı Tespit Algoritması

Birinci rapor “Büyük ihtimalle sahte BTS tarafından yakalanıldı” uyarısıdır. Bu uyarıyla MT’nin hizmet aldığı hücrenin büyük ihtimalle sahte BTS olduğu belirtilmektedir. İkinci rapor “Büyük ihtimalle ortamda sahte BTS var” uyarısıdır. Bu uyarıyla MT’nin hizmet aldığı hücre normal bir BTS olmakla birlikte komşu hücrelerden birisinin büyük ihtimalle sahte BTS olabileceği ve kısa bir zaman diliminde sahte BTS cihazının MT’yi ele geçirileceği tahmin edilmektedir. Üçüncü rapor ise “Sahte BTS’e yakalanılmış olabilir” uyarısıdır. Bu uyarıyla hizmet alınan BTS’in sahte BTS olabileceği konusunda şüpheler olduğu ifade edilmiştir.

Algoritmada karar verilmesini sağlayan 9 ana adım bulunmaktadır. Şekil 3.3’de gösterilen sahte BTS saldırı tespit algoritmasında da işaretlenen bu adımlar aşağıda detaylandırılmıştır.

1. Mühendislik modu etkin olan MT GSM ağ değerlerini okumaya başlar.
2. Cell ID, MCC, MNC, LAC, hizmet veren ve komşu hücreler gibi GSM ağ değerleri ve GSM ağ değerlerinden hesaplanmış C1 ve C2 parametreleri analiz ünitesine gönderilir.
3. Önceki bölümlerde açıklandığı gibi C2, ofset parametreleri değiştirilerek hücre seçimini etkilemek için kullanılabilmektedir. MT’nin BTS’e uzaklığını gösteren C1 parametresi yüksek olmasa bile, yani sahte BTS hedef MT’ye en yakın BTS olmasa bile sahte BTS, C2 değerini manipüle ederek MT’lerin kendine bağlanmasını sağlayabilmektedir. Önceki bölümlerde de bahsedildiği gibi sıra dışı bir durum olmadığında C1 ve C2 parametreleri yaklaşık olarak birbirine eşit çıkmaktadır. Bundan dolayı hizmet alınan hücrenin C2 ve C1 değerleri arasındaki farkın 25’den büyük olması, MT’nin sahte BTS’e yakalanmış olmasına yönelik güçlü işaretler vermektedir. 25 değeri hava arayüzünde yaşanması muhtemel bozulmaları ve hatalı-pozitif (false-positive) sonuçları elemek için deneysel olarak seçilmiştir.
4. Bu adım, küçük bir farkla üçüncü adımla aynı mantığa dayanmaktadır. Üçüncü adımda “hizmet verilen hücre sahte BTS mi?” sorusuna cevap verilirken bu adımda “komşu hücreler arasında sahte BTS var mı?” sorusuna cevap aranmaktadır. Kriterler bir önceki adım ile aynıdır.

5. İkinci bölümde de anlatıldığı gibi 3G ile birlikte karşılıklı doğrulama özelliği getirilmiş ve mevcut sahte BTS benzeri cihazlar çalışmaz olmuşlardır. Bu nedenle saldırganlar 3G BTS'leri sinyal bozucu ile bastırıp, MT'yi GSM kullanmaya zorlamaktadırlar. Bu nedenle ortamdaki 3G BTS'lerin kaybolup 2G BTS'lerin devam etmesi ortamda büyük ihtimalle sahte BTS olduğunu göstermektedir.
6. Önceki bölümlerde aktarıldığı gibi BTS'ler kendisini tanıtan bazı değerleri BCH'dan yayınlayacak şekilde yapılandırılmaktadır. Bu değerler arasında Cell ID, MCC, MNC, LAI ve komşu hücrelere ait bilgiler bulunmaktadır. Sahte BTS'in sahada kullanıldığı ve hareket halinde olduğu durumlarda komşu hücreler ve en zayıf hücre sürekli değişmekte ve saldırganın değişen komşu hücreleri güncellemesi zaman almaktadır. Eksik yapılandırılmış BTS için başka bir örnek ise sahte BTS için hiç var olmayan bir Cell ID seçilmesidir. Eğer bağlanılan BTS daha önceki BTS'lerin komşu hücreler listesinde yoksa bağlanılan hücre sahte BTS olabilir. Bunlara ek olarak, hizmet veren hücre o alanda yayın yapan tek hücre ise ve diğer komşu hücrelere ait değerler hizmet veren hücre tarafından yayınlanmıyorsa, diğer BTS'ler sinyal bozucu ile bastırılmış olup yalnızca bağlanılan sahte BTS'e izin verilmiş olunabilir.
7. Önceki bölümlerde anlatıldığı gibi LAI değişikliği MT'nin kimliğinin tespit edilmesi için gereklidir. MT'nin LAI bilgisi değişmediyse geliştirilen Algoritma mevcut hataların en kritiğini kullanıcıya bildirip, sonuca vardığı tüm uyarıları detaylı olarak raporlamalıdır. Sonrasında ise Algoritma birinci adımdan tekrar başlamalıdır. Eğer LAI bilgisi değiştiyse, inceleme devam etmelidir.
8. MT'nin hareket halinde olması ile bir lokasyon bölgesinden çıkılıp diğerine girilme ihtimali olduğundan kesin bir sonuca varılması mümkün değildir bu nedenle bir önceki adımdaki gibi Algoritma mevcut hataların en kritiğini kullanıcıya bildirip, sonuca vardığı tüm uyarıları detaylı olarak raporlamalıdır. Sonrasında ise Algoritma birinci adımdan tekrar başlamalıdır. Eğer MT sabitken LAI değişiyorsa şüpheli durum devam etmekte ve incelemeye devam edilmelidir.
9. MT'nin LAI bilgisinin değişimi ancak yeni bir BTS'e bağlanılması ile oluşabilmektedir. Eğer son bağlanılan BTS, komşu BTS'ler listesindeki en zayıf

BTS ise MT büyük ihtimalle sahte BTS'e yakalanmıştır. Eğer yeni bağlanılan BTS en zayıf BTS değilse ihtimal büyük olmamakla birlikte şüpheli bir durum olduğu anlaşılmakta ve MT'nin sahte BTS'e yakalanmış olma ihtimali olduğu anlaşılmaktadır.

Sonuç olarak, bahse konu senaryolar çeşitli alarmlar üretmektedir. Algoritmanın bir döngüsünde sadece bir alarm üretilebileceği gibi birden çok alarm da üretilebilmektedir. Algoritma devamlı çalışmalı ve karar yukarıda bahsedilen durumların hepsi göz önünde bulundurulduktan sonra verilmelidir. Bu durumun sağlanabilmesi için Algoritmada gösterilen "Çıkış" değişkeni kullanılmaktadır. Sahte BTS tespit algoritmasının yardımıyla, ortamda sahte BTS saldırısının tespitine yönelik alarmlar üretilmekte ve üretilen alarmlar saldırıya maruz kalınmış olunmasına dair önemli ipuçları vermektedir.

4. BULGULAR VE TARTIŞMA

Sahte BTS saldırı tespit algoritmasının gerçek ortamda test edilebilmesi için sahte BTS saldırısı yapan bir cihaza ihtiyaç duyulmaktadır. Söz konusu cihazın fiyatlarının karşılanabilecek seviyenin çok üstünde olması ve kullanımının illegal olmasından dolayı bir önceki bölümde detaylandırılan algoritmanın gerçek verileri kullanan simülasyonu yapılacaktır.

4.1 Uygulama Platformu

Üçüncü bölümde verilen sistem mimarisinin iki ana öğesi bulunmaktadır. Bunlar GSM sinyallerini analiz eden mühendislik modu etkin test telefonu ve analiz ünitesidir.

Bu kapsamda BTS'leri simüle etmek için kullanılan PC'nin ve simülasyon yazılımın platformu aşağıdadır.

- Windows 7 Ultimate
- Intel Core2 duo
- 3 GB Ram
- Java 1.7 (Swing)

GSM ağının okunup ilgili bilgilerin alınması için kullanılan cihazlar ve yazılımlara ait özellikler aşağıdadır

- Nokia N95
- Symbian v60
- Nokia Field Test

Geliştirilen sahte BTS saldırı tespit algoritması gelecek çalışmalarda benzetim yerine gerçek cihaz ile test edilebilme ihtimali göz önünde bulundurularak ANDROID işletim

sistemine uyumlu yazılmıştır. Algoritmayı koşan cihazın özelikleri ve cihaza ait kullanılan özellikler aşağıdadır.

- Google Nexus 4
- ANDROID 4.4.4 (Kit Kat)
- Wi-Fi Hotspot
- Entegre GPS modülü

4.2 Veri Kümesi

GSM verilerine yazılımsal yöntemlerle ulaşmak için hazır satılan ürünler bulunmaktadır. Ayrıca hâlihazırda günlük hayatta kullandığımız telefonlardan bazıları da söz konusu bilgilerin bir kısmını bilgilendirmek amaçlı kullanıcıya göstermektedir. Bu kapsamda Samsung, Apple, Nokia ve HTC marka telefonlardan bazı modeller incelenmiştir. İncelenen modellerden bazıları, GSM verilerinin -güvenlik nedenleriyle- sadece bir kısmını sağladıkları API ile kullanıcıya sunabilmektedirler. Örneğin ANDROID işletim sistemi kullanan akıllı telefonlar ve TelephonyManager API'si kullanılarak bağlı bulunan hücrenin Cell ID bilgisi, hücrenin sinyal seviyesi gibi bilgilere yazılımsal olarak erişilebilmekte ancak telefon tarafından hesaplanan C1 ve C2 değerleri gibi bilgilere ulaşılamamaktadır. Bununla birlikte, incelenen telefonlarda değişik isimlerde, değişik yöntemlerle ulaşılabilen mühendislik ekranları bulunmakta ve bu ekranlar aracılığıyla da bir kısım bilgilere görsel olarak ulaşılabilmektedir. Ulaşılan bilgiler markadan markaya ve telefondan telefona değişebilmekte olup, incelenen telefonlar arasında gözle ulaşılan veri miktarının en çok olduğu telefon modeli Nokia N95 olarak tespit edilmiştir.

Demo maliyetini düşürmek için GSM verilerine yazılımsal yöntemlerle erişebilme olanağı sağlayan hazır satılan ürünler yerine Nokia N95 ve üzerinde çalışan FieldTest uygulaması tercih edilmiş olup Fieldtest uygulaması ile ihtiyaç duyulan GSM ağ bilgileri temin edilmiştir. Söz konusu uygulamaya ait arayüzler şekil 4.1'de sunulmakta

olup uygulama tarafından elde edilen verilerin bir kısmı da arayüzlerde görülmektedir. Şekil 4.1'in;

- a bölümünde hizmet alınan hücreye ait genel bir özet ekranı yer almaktadır.
- b ve c'de hizmet alınan hücre ve komşu hücreler gibi MT'nin bilgilerini hesaplayıp kullandığı BTS'lere ait C1, C2, RX(sinyal seviyesi) gibi bilgiler bulunmaktadır.
- d bölümünde hizmet alınan hücreye ait MCC, MNC, LAI ve Cell ID bilgileri yer almaktadır.

Söz konusu yazılımın 100'e yakın ekranı bulunmakta ve bu ekranlardan ağ bilgilerini öğrenmenin yanı sıra MT'yi hücre seçimine zorlama gibi işlemler de yapılmaktadır.

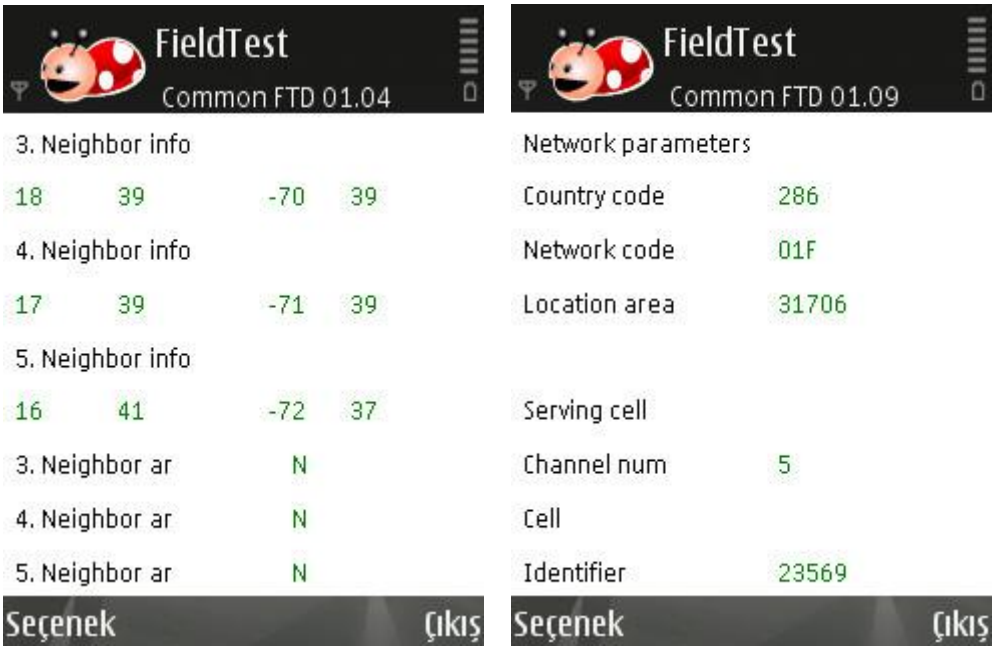
Yukarda bahsedilen FieldTest yazılımı Ankara ilinin çeşitli bölgelerinde Vodafone ve Turkcell operatörlerine ait BTS verilerine erişmek için çalıştırılmış ve Ankara'nın Macunköy semtinden elde edilen BTS verilere ait örnekler çizelge 4.1'de sunulmuştur.

Çizelge 4.1 Örnek BTS verileri

CellID	**MCC**	**MNC**	**LAI**	**C1**	**C2**	**NCEll_1**	**NCEll_2**	**NCEll_3**	**Operatör**
22239	**286**	**02**	**50637**	**38**	**38**	**22238**	**22236**	**22007**	**Vodafone**
22238	**286**	**02**	**50637**	**35**	**35**	**22239**	**22236**	**22214**	**Vodafone**
22236	**286**	**02**	**50637**	**34**	**34**	**22239**	**22238**	**22214**	**Vodafone**
37430	**286**	**01**	**31706**	**47**	**47**	**46156**	**23574**	**8550**	**Turkcell**
46156	**286**	**01**	**31706**	**41**	**40**	**37430**	**23574**	**8550**	**Turkcell**
23574	**286**	**01**	**31706**	**38**	**38**	**37430**	**46156**	**8550**	**Turkcell**
8550	**286**	**01**	**31706**	**34**	**34**	**37430**	**46156**	**23574**	**Turkcell**

Geliştirilen Algoritma yukarda örnekleri gösterilen FieldTest uygulaması verileriyle çalıştırılmış olup, Algoritmanın test edilebilmesi için saldırı içerikli sahte BTS verileri de üretilip sistemde kullanılmıştır.

a) b)

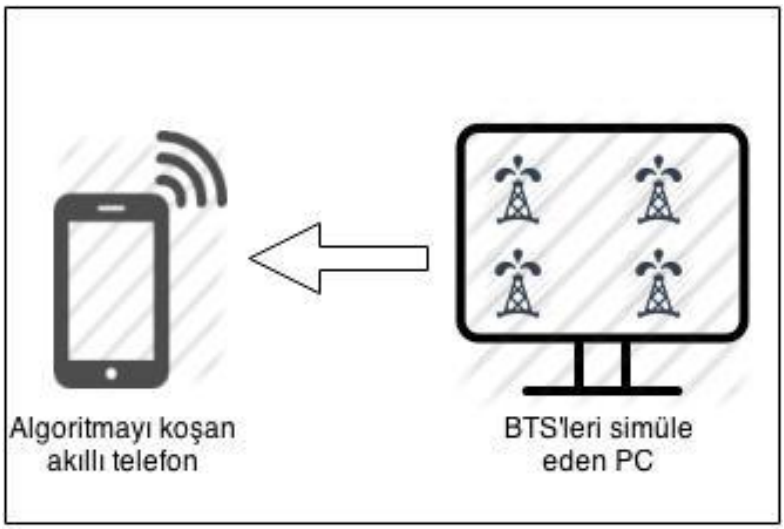


c) d)

Şekil 4.1 FieldTest arayüzleri

4.3 Geliştirilen sahte BTS saldırı tespit algoritması

Simülasyon için kullanılan PC, FieldTest programından aldığı verileri ve üretilen diğer BTS bilgilerini, geliştirilen yazılımla akıllı telefona göndermektedir. Söz konusu BTS verileri gönderilirken PC ve akıllı telefon arasında soket bağlantısı kullanılmaktadır. Algoritmayı koşan akıllı telefon ise söz konusu BTS'lerin son hallerine ait bilgileri değerlendirmekte ve çıkardığı özet bilgileri saklamaktadır. PC ile akıllı telefon arasındaki bağlantı akıllı telefonlarda bulunan Wifi Hotspot teknolojisi kullanılarak sağlanmıştır. Wifi Hotspot kullanım kolaylığı için seçilmiş olup bağlantı, kullanılması planlanan mimariye göre değiştirilebilmektedir. Simülasyonun için seçilen mimari şekil 4.2'de sunulmaktadır.

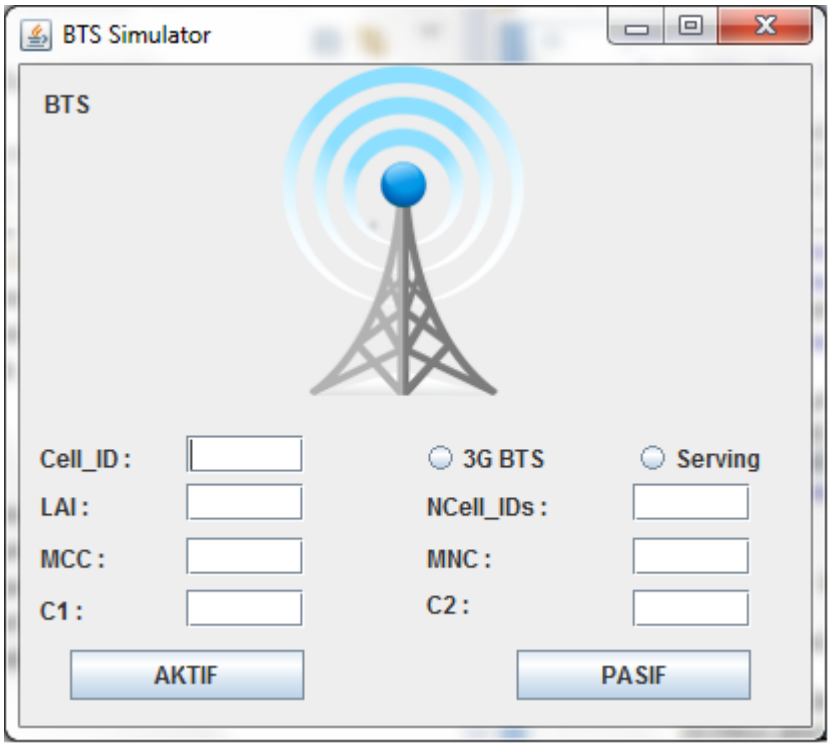


Şekil 4.2 Simülasyon mimarisi

Simülasyon, algoritmayı çalıştıran akıllı telefon tarafında yapılabilecek olmasına rağmen verilerin ayrılması ve algoritmanın her türlü veri kaynağı ile çalışabilmesi için bir protokol geliştirilmiştir. Şekil 4.3'de gösterilen yazılım söz konusu protokole göre verileri algoritmayı koşan akıllı telefona göndermektedir.

Algoritmadaki önemli parametrelerden birisi de MT'nin hareket halinde olup olmadığıdır. MT'nin hareketi ile ilgili bilgi demo sisteminde kullanılan akıllı telefonun

entegre GPS modülü kullanılarak hesaplanmaktadır. İki döngü arasındaki ortalama hız hesaplanıp 10 km/s hızın altındaysa MT hareket etmiyor kabul edilmektedir. Eğer akıllı telefon kapalı alanda bulunup GPS uydularına erişilememesi gibi bir sebeple konum bilgisine erişemeyip ortalama hız hesaplanamıyorsa, MT hareket halinde kabul edilmektedir.



Şekil 4.3 BTS simülasyon yazılımına ait ekran görüntüsü

Algoritmadaki "3G/4G BTS'ler sinyal vermez oldular mı" koşulu için bir önceki döngüde en az 2 tane 3G BTS'den sinyal alınamıyorsa ilgili koşul değerlendirme dışı kalacaktır aksi halde kırsal alanlarda kapsama alanında olan BTS sayısı oldukça kısıtlı olduğundan yanlış-alarm (false-positive) oranının artması kaçınılmazdır.

Algoritmadaki "Hizmet veren hücre eksik bilgiler yayınlıyor mu?" koşulu için sadece MCC, MNC ve komşu hücre listesi değerlerine bakılmış olup, MCC ve MNC bilgilerinin hizmet alınan operatörle uyumlu, komşu hücre listesi bilgilerinde ise en az iki tane komşu hücre bilgisinin yer alması beklenmiştir.

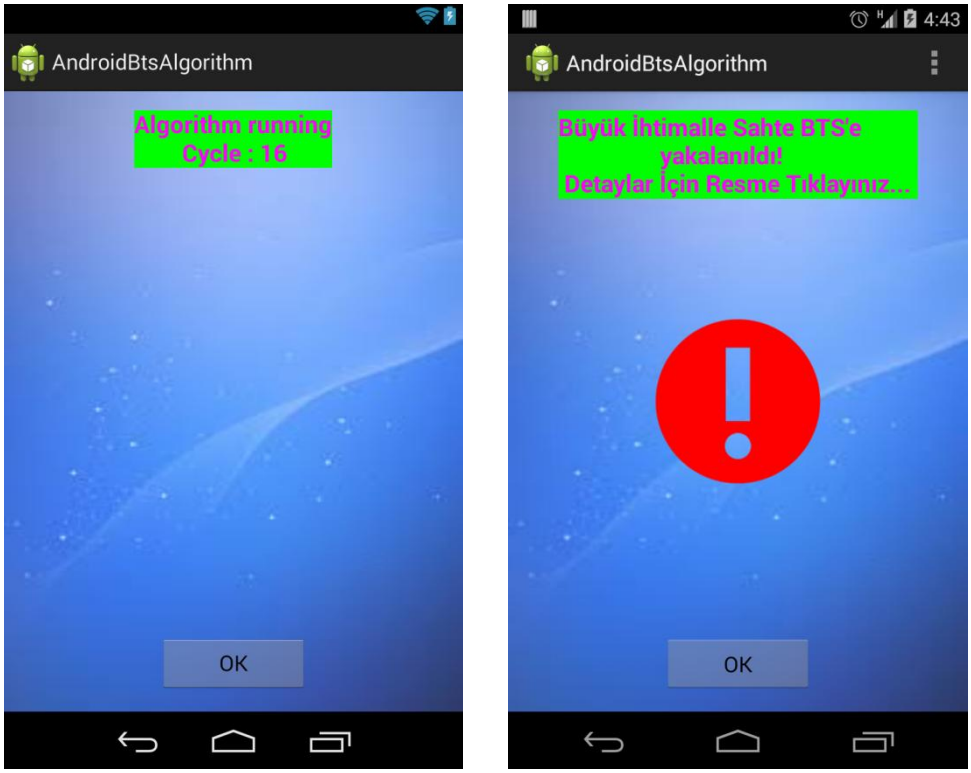
Algoritmayı çalıştıran ANDROID uygulaması periyodik olarak çalışmakta ve PC tarafından simüle edilen BTS'lerin bilgilerini okumaktadır. Sonrasında, uygulama BTS'den gelen verileri algoritmaya ve yukarıda anlatılan kabullere göre değerlendirmekte ve alarmları oluşturmaktadır. Eğer birden çok alarm üretildiyse, uygulama en ciddi olanı ekranda uyarı olarak gösterip diğerlerini de bilgi olarak detay kısmında raporlamaktadır. Algoritmanın döngüleri dakikada bir çalışmaktadır. Her döngüde önce simüle edilen BTS verileri okunmakta, sonrasında akıllı telefonun dâhili GPS modülü kullanılarak lokasyon değişikliği ve ortalama hız hesaplanmaktadır. Ayrıca okunan bu değerlerden bazıları bir sonraki döngü için saklanmakta ve güncel döngü verileri ile beraber değerlendirilip sonuç üretilmektedir.

Akıllı telefonda çalışan sahte BTS tespit algoritması önceki bölümlerde anlatılan durumlarla karşılaştığında 3 şekilde uyarıda bulunmaktadır. Birincisi, "yüksek ihtimalle sahte BTS'e yakalandınız" uyarısıdır. Bu uyarıyla kullanıcı, MT'nin hizmet aldığı hücre büyük ihtimalle sahte BTS olduğunu ve büyük ihtimalle sahte BTS cihazı tarafından yapılan saldırıya maruz kaldığını anlamalıdır. İkincisi, "yüksek ihtimalle ortamda sahte BTS çalışmaktadır" uyarısıdır. Kullanıcı bu uyarıyla, komşu hücrelerden birisinin büyük ihtimalle sahte BTS olduğunu ve kullandığı MT'nin sahte BTS'e yakalanmak üzere olduğunu düşünebilir. Üçüncüsü, "sahte BTS'e yakalanılmış olabilir" uyarısıdır. Bu uyarıda ise hizmet alınan hücrenin sahte BTS olma ihtimali vardır ve kullanıcı daha yüksek seviyeli bir uyarı için hazırlıklı olmalıdır. Algoritmanın çalışma döngüsü olarak bir dakika seçilmiştir, çünkü ikinci bölümde bahsedilen çalışmalardan en başarılı olan sahte BTS saldırısının telefonların çoğunu yakalaması yaklaşık 40 saniye sürmüştür.

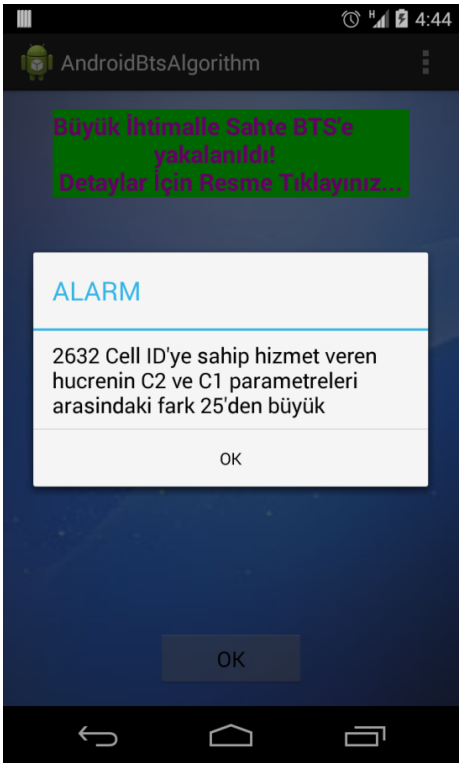
ANDROID uygulamasının ürettiği alarmlara ait ekran görüntüleri şekil 4.4'de sunulmaktadır. Şekil 4.4.a'da algoritma çalışmakta ve kaçıncı döngüde olduğunu kullanıcıya iletmektedir. Şekil 4.4.b'de algoritma olağan dışı bir durumla karşı karşıya kalıp uyarı vermiştir. Uyarının seviyesine göre kırmızı sarı ve yeşil alarmlar üretilmektedir. Şekil 4.4.c'de ise uyarı ikonunun üzerine tıklanmış ve uyarı detay ekranı açılmıştır. Bu ekranda uyarının detayları ve daha az kritik olan uyarılar görüntülenmektedir.

Tespit algoritmasının dakikada bir defa çalıştırılmasıyla mevcut saldırıların kaçırılmaması sağlanmaya çalışılmıştır. Algoritmanın gerçek sahte BTS cihazı ile test edilmesi ve BTS bilgilerinin gerçek zamanlı okunabilmesi durumunda, GSM protokolünde BCH'ın okunması için maksimum süre 5 sn. olduğundan uygulamanın daha kısa periyotlarla çalıştırılması gerekecektir.

Akıllı telefon tarafında çalışan sahte BTS saldırı tespit algoritmasını koşan ANDROID uygulamasına ait kod örneği Ek 1'de, baz istasyonlarını simüle eden PC yazılımına ait kod örneği ise Ek 2'de sunulmuştur.



a) b)



c)

Şekil 4.4 Algoritma uygulamasına ait ekran görüntüleri.

5. TARTIŞMA VE SONUÇ

GSM Dünya çapında en yaygın kullanılan mobil iletişim sistemi olup yaklaşık 7 milyar aboneliğe sahiptir. Temel haberleşmeden ticari uygulamalara kadar neredeyse her alanda kullanılan GSM konuşma ve kişisel internet verisi gibi kişisel bilgi güvenliği için bir hayli önemli olan verileri taşımaktadır.

GSM'in yaygın kullanımına rağmen GSM'de bir takım güvenlik açıkları bulunmaktadır. Söz konusu açıkların mevcut mimari üzerinde değişiklik yapılarak yamanması teorik olarak mümkün olsa da bütün BTS'lerin ve SIM'lerin değişmesi gerektiğinden ticari olarak mümkün görünmemektedir.

GSM'de bulunan açıklardan en kritiklerinden birisi olan BTS ve MT arasında karşılıklı doğrulamanın eksikliği, ikinci bölümde de detaylı anlatıldığı gibi man-in-the-middle saldırılarına kapı aralamaktadır. Man-in-the-middle saldırılarını temel alan sahte BTS cihazları ile en basitinden MT'nin kimliğinin ele geçirilmesi yapılabileceği gibi tele kulak ve MT'nin yerinin tespit edilip silahlı saldırı yapılması gibi tehlikeli saldırılar da yapılabilmektedir.

Karşılıklı doğrulama eksikliğinin bu denli kritik sonuçları olması, sahte BTS cihazlarının tespit edilmesini önemli kılmaktadır. Literatür taramalarında sahte BTS cihazının geliştirilmesine yönelik çalışmalar bulunmasına rağmen bu cihazların tespit edilmesine yönelik çalışmaya rastlanmaması yapılan çalışmanın önemini artırmaktadır.

Tez çalışmasında öncelikle GSM mimarisi analiz edilmiş olup karşılıklı doğrulama açığına neden olan ilgili GSM protokolleri de detaylandırılmıştır. Sonrasında sahte BTS saldırıları ile ilgili literatür çalışması yapılıp saldırı teknikleri ve birbirlerine göre üstün tarafları ele alınmıştır. Üçüncü bölümde sahte BTS saldırılarının tespit edilmesi için bir algoritma önerilmiş olup dördünce bölümde geliştirilen algoritmanın fonksiyonalitesini ve uygulanılabilirliğini gösteren simülasyon yapılıp algoritmanın gösterimi yapılmıştır.

Geliştirilen algoritma sahte BTS cihazı temin edilemediğinden BTS simülasyonu ile test edilmiştir. Söz konusu cihazın sahte BTS cihazı ile test edilmesine müteakip çalışma tez çalışması ürün haline getirilebilecektir.

Mobil iletişim sürekli değişmekte ve yenilenmekte olup gün geçtikçe GSM için var olan açıklar 3G ve 4G için de ortaya çıkmaktadır. GSM için yapılan güvenlik analizleri tespit edilip gerekli önlemlerin alınması yeni gelişen mobil iletişim ağları için de yapılması çalışmanın bir sonraki adımı olarak planlanmıştır.

KAYNAKLAR

Anonymous. 1992. European Digital cellular telecommunications system Phase , Location Registration Procedures. (GSM 03.12-DCS version 3.0.1 Release 1992).

Anonymous. 1998. Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode. (GSM 03.22 version 5.3.1 Release 1996)," Document ETSI 300 930

Anonymous. 1999. Digital cellular telecommunications system (Phase 2+); Radio subsystem link control. (GSM 05.08 version 8.5.0 Release 1999), Document ETSI TS 100 911 V8.5.0 (2000-10).

Anonymous. 2014a. Web Sitesi: http://en.wikipedia.org/wiki/GSM, Erişim Tarihi: 15.08.2014.

Anonymous. 2014b. Web Sitesi: http://www.gsm-history.org, Erişim Tarihi: 14.08.2014.

Anonymous. 2014c. Web Sitesi: http://w ww.gsma.com, Erişim Tarihi: 17.08.2014.

Anonymous. 2014d. Web Sitesi: http://www.technologyuk.net/telecommunications/communication_technologies/gsm.shtml, Erişim Tarihi: 28.11.2014.

Anonymous. 2014e. Web Sitesi: http://www.septier.com/368.html, Erişim Tarihi: 28.11.2014.

Ahmadian, Z., Salimi, S. and Salahi, A. 2010. Security Enhancements againts UMTS-GSM interworking attacks, Computer Networks ,(54), 2256-2270.

Borgaonkar, R. ve Udar, S. 2014. Web Sitesi: https://www.isti.tuberlin.de/fileadmin/fg214/ravi/ Darshak-bh14.pdf, Erişim Tarihi: 02.12.2014

Broek, F.V.D. 2010. Eavesdropping on GSM: State-of-affairs. 5th Benelux Workshop on Information and System Security (WISSec), Kasım 2010, Radboud University, Nijmegen.

Garg, V. K. and Wilkes J. E. 1998. Principles and Applications of GSM. Prentice Hall, 512, New Jersey.

González-Castaño, J.F., Vales-Alonso, J. J., Pousada-Carballo, M., Isasi de Vicente, F. and Fernández-Iglesias, M.J. 2002. Real-Time Interception Systems for the GSM Protocol, IEEE Transactions on Vehicular Technology, vol. 51, no. 5.

Heine, G., 1998. GSM Networks: Protocols, Terminology, and Implementatıon. Artech House, 417, London.

Kahabka, M. 2014. Web Sitesi: http://web.itu.edu.tr/~pazarci/Wandel Goltermann_gsm.pdf, Erişim Tarihi: 02.12.2014.

Kalenderi, M., Pnevmatikatos, D., Papaefstathiou, I. and Manifavas, C. 2012. Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAS. 22nd International FPL Conference, 29-31 Aug. , Field Programmable Logic and Applications (FPL) Conference, 747-753, Oslo.

Meyer, U. and Wetzel, S. 2004. On the Impact of GSM Encryption and Man-In-The-Middle Attacks on the Security of Interoperating GSM/UMTS Networks. Personal, Indoor and Mobile Radio Communications(PIMRC 2004), 5-8 Sept. Darmstadt Univ. of Technol. 2876-2883, Germany.

Ntantigian, C. and Xenakis, C. 2011, Questioning the Feasibility of UMTS-GSM Interworking Attacks. Wireless Pers Commun (2012) 65:157–163, DOI 10.1007/s11277-011-0233-7

Pousada-Carballo, J.M., González-Castaño, F. J., Vicente, F. I. and Fernández-Iglesias M.J. 1998. Jamming system for mobile communications. Electron. Lett. vol. 34, pp. 2166–2167.

Scahill J. and Greenwald G. 2014. https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/ Erişim Tarihi : 16.08.2014.

Song, Y., Zhou, K and Chen, X. 2012. Fake BTS Attacks of GSM System on Software Radio Platform. Journal of Networks, vol. 7, no. 2.

Vales-Alonso, J., Vicente, F. I., González-Castaño, F. J., and Pou-sada-Carballo, J.M. 2001. Real-time detector of GSM terminals. IEEE Commun.Lett., vol. 5, pp. 275–276.

Zhou, K., Hu, A. and Song, Y. 2010. A No-Jamming Selective Interception System of the GSM Terminal" 6th International Conference on Wireless Communications Networking & Mobile Computing (WiCOM), p1-4.

EKLER

EK 1 Sahte Baz İstasyonu Saldırı Tespit Algoritması Kod Örneği

EK 2 Baz İstasyonu Simülasyon Yazılımı Kod Örneği

EK 1 Sahte Baz İstasyonu Saldırı Tespit Algoritması Kod Örneği

```
package com.omer.faruk.celik.algorithm;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.net.ServerSocket;
import java.net.Socket;
import java.util.ArrayList;
import java.util.Collections;
import java.util.Iterator;
import java.util.List;
import java.util.Timer;
import java.util.TimerTask;
import android.app.Activity;
import android.location.Location;
import android.location.LocationListener;
import android.location.LocationManager;
import android.os.Bundle;
import android.os.Handler;
import android.util.Log;
import android.widget.TextView;

public class Server extends Activity {
        private ServerSocket serverSocket;
        public Handler updateUIHandler;
        Thread serverThread = null;
        private TextView text;
        public List<BTS> btsList = new ArrayList<BTS>();
        public BTS lastWeakestBTS;
        public BTS servingCell;
        public int last3GBTSCount = 0;
        public int lastLAI = 0;
        LocationManager locManager;
```

```
	Location lastLocation;
	int cycleCounter = 0;
	List<Warning> warningList;
	List<Warning> allWarnings;
	List<Warning> displayWarnings;
	public static final int SERVERPORT = 6060;

	@Override
	public void onCreate(Bundle savedInstanceState) {
		super.onCreate(savedInstanceState);
		setContentView(R.layout.main);
		locManager = (LocationManager)
getSystemService(getBaseContext().LOCATION_SERVICE);
		text = (TextView) findViewById(R.id.text2);
		updateUIHandler = new Handler();
	allWarnings = new ArrayList<Warning>();
	Thread algThread = new Thread(new Algorithm());
	serverThread = new Thread(new ServerThread());
	serverThread.start();
	algThread.start();
}

/** Algoritmayi kosan sinifdir, Periyodik calisir
 *
 * @author OFC
 *
 */
class Algorithm implements Runnable {
	private static final long DELAY = 0;
	private static final long ONE_MINUTE = 1000 * 60;

	public void run() {
		final Timer timer = new Timer();

		timer.scheduleAtFixedRate(new TimerTask() {
```

```
                @Override
                public void run() {
                        warningList = new ArrayList<Warning>();
                        int bts3GCounter = 0;

//                                      updateConversationHandler.post(new
updateUIThread(counter
//                                                              .toString()));
Log.i("Algorithm", "cycleCounter is: " + cycleCounter);
cycleCounter++;
// Hizmet veren hucrenin c1 ve C2 degerini kontrol et
Log.i("Algorithm", "Serving cell's C1 and C2");

if (servingCell == null) {
        Log.e("Algorithm",
"Serving cell is not exists. Aborting!!");
        raporla();
        return;
} else if (Math.abs(servingCell.c2Parameter
                - servingCell.c1Parameter) > 25) {
        warningList
                        .add(new Warning(
                                        3,
                                        servingCell.cell_IDParameter,
                                        "Hizmet veren hucrenin C2 "
+ "ve C1 degerleri arasindaki fark 25'den fazla "));
}
// En guclu 6 baz istasyonuna bakiliyor eger C2 ve C1
// degerleri arasindaki fark 25 den fazla ise uyari
// veriliyor
Log.i("Algorithm", "Neighbour CEll's C1 and C2");
for (int i = 0; i < 6; i++) {
        if(btsList.get(i) == null)
                break;
```

```
		if (Math.abs(btsList.get(i).c2Parameter
					- btsList.get(i).c1Parameter) > 25) {
			warningList
					.add(new Warning(
							2,
							btsList.get(i).cell_IDParameter,
							btsList.get(i).cell_IDParameter
									+ " id numarali "
+ "hucrenin C2 ve C1 degerleri arasindaki fark 25'den fazla "));
Log.i("Algorithm",
btsList.get(i).cell_IDParameter
			+ " id numarali "
+ "hucrenin C2 ve C1 degerleri arasindaki fark 25'den fazla ");
			break;
		}
}
// 3G BTS'lerin yok olup olmadigi kontrol edilsin
Iterator<BTS> it = btsList.iterator();
while (it.hasNext()) {
		if (it.next().bts3GParameter)
			bts3GCounter++;
}
Log.i("Algorithm", "Number of 3G BTS is " + bts3GCounter);
if (last3GBTSCount >= 2 && bts3GCounter == 0) {
		warningList.add(new Warning(2, 0, last3GBTSCount
					+ " tane  3G BTS yok olmustur"));
Log.i("Algorithm", last3GBTSCount
+ " tane  3G BTS yok olmustur");
}
// last3GBTSCount degerini guncelle
last3GBTSCount = bts3GCounter;

// Komsu hucrelerden eksik deger yayan var mi onu kontrol
// et.
for (int i = 0; i < 6; i++) {
```

```
        if (btsList.get(i).MCCParameter == 0
                        || btsList.get(i).MNCParameter == 0
                        || btsList.get(i).nCellsParameter == false) {
                warningList
                                .add(new Warning(
                                                1,
                                                btsList.get(i).cell_IDParameter,
                                                btsList.get(i).cell_IDParameter
                                                                + "cellID'ye sahip hucre eksik
bilgiler yayinlamaktadir."));
        }
}

// LAI degisti mi kontrol et, degismediyse raporlamaya gec
if (servingCell.LAIParameter != lastLAI) {
        // MT hareket halinde mi GPS lokasyonundan ogren
locManager.requestLocationUpdates(
                LocationManager.GPS_PROVIDER, 1000L, 500.0f,
                locationListener);
Location location = locManager
                .getLastKnownLocation(LocationManager.GPS_PROVIDER);
if (location == null) {
        raporla();
        Log.i("Algorithm",
"lokasyon alinamadi. Raporlaniyor... ");
        return;
}
if (lastLocation == null) {
        lastLocation = location;
        raporla();
        Log.i("Algorithm",
"ilk defa lokasyon alindi. Raporlaniyor. ");
        return;
}
```

```
// mesafe ve zaman hesapla
double distanceInKm = location.distanceTo(lastLocation) / 1000;
long timeInHours = (location.getTime() - lastLocation
                .getTime()) / (1000 * 60 * 60);
// if MT is moving
if (distanceInKm / timeInHours < 10) {
        //MT is not moving
if (lastWeakestBTS == null) {
        raporla();
        Log.i("Algorithm", "En zayif BTS null ");
        return;
} else if (servingCell.cell_IDParameter == lastWeakestBTS.cell_IDParameter) {
        // en zayif bts'e baglandi mi?
warningList
                .add(new Warning(
                                3,
                                servingCell.cell_IDParameter,
                                " servingCell.cell_IDParameter id numarali "
+ "hucrenin bir onceki durumda en zayif hucreydi "));
Log.i("Algorithm"," servingCell.cell_IDParameter id numarali "
+ "hucrenin bir onceki durumda en zayif hucreydi ");
        raporla();
        return;
} else {
        // en zayif bts'e baglanilmadi
warningList
.add(new Warning(
                1,
                servingCell.cell_IDParameter,
                " LAI degisti ve MT hareket halinde degil "));
Log.i("Algorithm","      LAI degisti ve MT hareket halinde degil ");
                raporla();
                return;
        }
```

```
}else {
        //MT hareket halinde, karar verilemez
Log.i("Algorithm"," MT hareket halinde degil ");
                                        raporla();
                                        return;
                                }
                        }
                }
        }
        , DELAY, ONE_MINUTE);
}
private void raporla() {
        displayWarnings = new ArrayList<Warning>();
        int highestWarningLevel = 0;
        // last LAI degistir
lastLAI = servingCell.LAIParameter;
// Weakest BTS degistir
if (!btsList.isEmpty() ) {
        for (int i = 0; i < 6; i++) {
                if(btsList.get(i) == null) {
                        lastWeakestBTS = btsList.get(i-1);
                        break;
                }
        }
}else
        Log.e("Algorithm", "There is no active neighbor cells");

if (!warningList.isEmpty()) {
        //yeni bir goruntuleme warning listesi olustur ve hepsini kopyala
        Iterator<Warning> it = warningList.iterator();
        while (it.hasNext()) {
                displayWarnings.add(it.next());
                allWarnings.add(it.next());
                if(it.next().warningLevel > highestWarningLevel)
                        highestWarningLevel = it.next().warningLevel;
```

```
            }
            updateUIHandler.post(new updateUIThread(highestWarningLevel, displayWarnings));

}else {
            Log.i("Algorithm","There is no warnings in cycle :" + cycleCounter );
                        }




            }
}
@Override
protected void onStop() {
            super.onStop();
            try {
                        serverSocket.close();
            } catch (IOException e) {
                        e.printStackTrace();
            }
}
private void updateWithNewLocation(Location location) {
            // TextView myLocationText = (TextView) findViewById(R.id.text);
String latLongString = "";
if (location != null) {
            double lat = location.getLatitude();
            double lng = location.getLongitude();
            latLongString = "Lat:" + lat + "\nLong:" + lng;
} else {
            latLongString = "No location found";
}
// myLocationText.setText("Your Current Position is:\n" +
// latLongString);
}
private final LocationListener locationListener = new LocationListener() {
            public void onLocationChanged(Location location) {
```

```
                updateWithNewLocation(location);
        }
        public void onProviderDisabled(String provider) {
                updateWithNewLocation(null);
        }

        public void onProviderEnabled(String provider) {
        }
        public void onStatusChanged(String provider, int status, Bundle extras) {
        }
};

/** Algoritmanin urettigi alarmlari tutar
 *
 * @author OFC
 *
 */
class Warning {
        int warningLevel = 0;
        int warningCellID;
        String warningText;
        Warning(int warningLevel, int warningCellID, String warningText) {
                this.warningLevel = warningLevel;
                this.warningCellID = warningCellID;
                this.warningText = warningText;
        }
}
class ServerThread implements Runnable {
        public void run() {
                Socket socket = null;
                try {
                        serverSocket = new ServerSocket(SERVERPORT);
                } catch (IOException e) {
                        e.printStackTrace();
                }
```

```
                while (!Thread.currentThread().isInterrupted()) {

                        try {
                                socket = serverSocket.accept();
                                CommunicationThread commThread = new
CommunicationThread(
                                                socket);
                                new Thread(commThread).start();
                        } catch (IOException e) {
                                e.printStackTrace();
                        }
                }
        }
}
/** Socket server olarak calisir ve gelen BTS ekleme silme islemlerini yapar
 *
 * @author OFC
 *
 */
class CommunicationThread implements Runnable {
        private Socket clientSocket;
        private BufferedReader input;

        public CommunicationThread(Socket clientSocket) {
                this.clientSocket = clientSocket;
                try {
                        this.input = new BufferedReader(new InputStreamReader(
                                        this.clientSocket.getInputStream()));
                } catch (IOException e) {
                        e.printStackTrace();
                }
        }
        public void run() {
                while (!Thread.currentThread().isInterrupted()) {
                        try {
```

```
                                        String read = input.readLine();
                                        String[] parts = read.split(",");
// hizmet veren hucreyi ayri tutmamiz gerekecek
if (parts[9].equals("true")) {
servingCell = new BTS(Integer.parseInt(parts[1]),
                        Integer.parseInt(parts[2]),
                        Integer.parseInt(parts[3]),
                        Integer.parseInt(parts[4]),
                        Integer.parseInt(parts[5]),
                        Integer.parseInt(parts[6]), parts[7].isEmpty(),
                        parts[8].equals("True"),
parts[9].equals("True"));
}
// BTS sil
if (parts[0].equals("00000")) {
Iterator<BTS> it = btsList.iterator();
while (it.hasNext()) {
            if (it.next().cell_IDParameter == Integer
                                    .parseInt(parts[1])) {
                        it.remove();
                        // If you know it's unique, you could `break;`
// here
            }
}
// yeni BTS
} else if (parts[0].equals("11011")) {
btsList.add(new BTS(Integer.parseInt(parts[1]), Integer
                        .parseInt(parts[2]),
                        Integer.parseInt(parts[3]), Integer
                                        .parseInt(parts[4]), Integer
                                        .parseInt(parts[5]), Integer
                                        .parseInt(parts[6]),
                        parts[7].isEmpty(), parts[8].equals("True"),
parts[9].equals("True")));
//sort the bts list according to C1 value;
```

```
            Collections.sort(btsList);
}
// updateConversationHandler.post(new updateUIThread(read));

                                } catch (IOException e) {
                                        e.printStackTrace();
                                }
                        }
                }
}
class updateUIThread implements Runnable {
            private int warningLevel;
            private List<Warning> displayWarningList;
            public updateUIThread(int warningLevel, List<Warning> displayWarnings) {
                        this.warningLevel = warningLevel;
                        this.displayWarningList = displayWarnings;
            }
            @Override
            public void run() {
                        text.setText(text.getText().toString() + "Client Says: " + warningLevel
+ "\n");
                        }
            }
/**
 * BTS class
 * Created by OFC on 07.12.2014.
 */
public class BTS  implements Comparable<BTS>{
   int cell_IDParameter;
   int MCCParameter;
   int MNCParameter;
   int LAIParameter;
   int c1Parameter;
   int c2Parameter;
   boolean nCellsParameter;
   boolean bts3GParameter;
   boolean aktif;
   boolean serving;


   public int getC1Parameter() {
```

```
        return c1Parameter;
    }



    public BTS(int cell_IDParameter, int MCCParameter, int MNCParameter, int LAIParameter,
int c1Parameter,
            int c2Parameter, boolean nCellsParameter, boolean bts3GParameter, boolean serving)
{
        this.cell_IDParameter = cell_IDParameter;
        this.MCCParameter = MCCParameter;
        this.MNCParameter = MNCParameter;
        this.LAIParameter = LAIParameter;
        this.c1Parameter = c1Parameter;
        this.c2Parameter = c2Parameter;
        this.nCellsParameter = nCellsParameter;
        this.bts3GParameter = bts3GParameter;
        this.serving = serving;
        this.aktif = true;
    }

            @Override
            public int compareTo(BTS compareBTS) {
        int c1compare=((BTS)compareBTS).getC1Parameter();
        /* For descending order*/
        return c1compare - this.c1Parameter;
    }

}
```

EK 2 Baz İstasyonu Simülasyon Yazılımı Kod Örneği

```
import java.awt.EventQueue;
public class Test_Swing extends JFrame {
	private JPanel contentPane;
	private JTextField CellID_Text;
	private JTextField LAI_Text;
	private JTextField MCC_Text;
	private JTextField NCell_ID_Text;
	private JTextField MNC_Text;
//	private JTextField C1_Text;
//	private JTextField C2_Text;
private JLabel lblNcellid;
private JLabel lblMnc;
private JLabel lblNewLabel;
private final Action action = new SwingAction();

/**
 * Launch the application.
 */
private Socket socket;
  private static final int SERVERPORT = 6060;
  private static final String SERVER_IP = "192.168.43.6";
  private JLabel c1_Label;
  private JTextField C1_Text;
  private JLabel C2_Label;
  private JTextField C2_Text;
  private JRadioButton radio_btn_3G;
  private JButton btnPasif;
  private JRadioButton radioBtnServing;
public static void main(String[] args) {
	EventQueue.invokeLater(new Runnable() {
		public void run() {
			try {
				Test_Swing frame = new Test_Swing();
				frame.setVisible(true);
			} catch (Exception e) {
				e.printStackTrace();
			}
		}
	});
}
class ClientThread implements Runnable {
	@Override
	public void run() {
		// TODO Auto-generated method stub
InetAddress serverAddr;
try {
	serverAddr = InetAddress.getByName(SERVER_IP);
	socket = new Socket(serverAddr, SERVERPORT);
} catch (UnknownHostException e) {
	// TODO Auto-generated catch block
```

```
			e.printStackTrace();
		} catch (IOException e) {
			// TODO Auto-generated catch block
					e.printStackTrace();
				}
			}
		}
		/**
		 * Create the frame.
		 */
		public Test_Swing() throws IOException {
			this.setTitle("BTS Simulator");
		setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
		setBounds(100, 100, 411, 368);
		contentPane = new JPanel();
		contentPane.setBorder(new EmptyBorder(5, 5, 5, 5));
		setContentPane(contentPane);
		contentPane.setLayout(null);

		JLabel btsPicLabel = new JLabel();
		btsPicLabel.setBounds(0, 0, 383, 166);
		btsPicLabel.setHorizontalAlignment(SwingConstants.CENTER);
		contentPane.add(btsPicLabel);

		ImageIcon imgThisImg = new ImageIcon("bts1.png");
		btsPicLabel.setIcon(imgThisImg);

		JLabel lblNewLabel_1 = new JLabel("Cell_ID :");
		lblNewLabel_1.setBounds(10, 189, 70, 15);
		contentPane.add(lblNewLabel_1);

		CellID_Text = new JTextField();
		CellID_Text.setBounds(83, 185, 59, 19);
		contentPane.add(CellID_Text);
		CellID_Text.setColumns(10);

		JLabel lblLac = new JLabel("LAI :");
		lblLac.setBounds(10, 213, 70, 15);
		contentPane.add(lblLac);

		JLabel lblMcc = new JLabel("MCC :");
		lblMcc.setBounds(10, 239, 70, 15);
		contentPane.add(lblMcc);

		LAI_Text = new JTextField();
		LAI_Text.setColumns(10);
		LAI_Text.setBounds(83, 209, 59, 19);
		contentPane.add(LAI_Text);

		MCC_Text = new JTextField();
		MCC_Text.setColumns(10);
		MCC_Text.setBounds(83, 236, 59, 19);
		contentPane.add(MCC_Text);
```

```
NCell_ID_Text = new JTextField();
NCell_ID_Text.setColumns(10);
NCell_ID_Text.setBounds(306, 209, 59, 19);
contentPane.add(NCell_ID_Text);

MNC_Text = new JTextField();
MNC_Text.setColumns(10);
MNC_Text.setBounds(306, 236, 59, 19);
contentPane.add(MNC_Text);

lblNcellid = new JLabel("NCell_IDs :");
lblNcellid.setBounds(203, 213, 70, 15);
contentPane.add(lblNcellid);

lblMnc = new JLabel("MNC :");
lblMnc.setBounds(203, 239, 70, 15);
contentPane.add(lblMnc);

lblNewLabel = new JLabel("BTS");
lblNewLabel.setBounds(12, 12, 70, 15);
contentPane.add(lblNewLabel);
JButton btnAktif = new JButton("AKTIF");
btnAktif.addActionListener(new ActionListener() {
	public void actionPerformed(ActionEvent arg0) {
		// Gonderilen string 11011 ile basliyorsa aktif 00000 ile basliyorsa pasif
SendDataToServer("11011",CellID_Text.getText(),LAI_Text.getText(),
NCell_ID_Text.getText(),MNC_Text.getText(),MCC_Text.getText()
,C1_Text.getText(),C2_Text.getText(),radio_btn_3G.isSelected());
//					System.out.println(LAC_Text.getText());
	}

});
btnAktif.setAction(action);
btnAktif.setBounds(25, 292, 117, 25);
contentPane.add(btnAktif);

btnPasif = new JButton("PASIF");
btnPasif.addActionListener(new ActionListener() {
	public void actionPerformed(ActionEvent arg0) {
		SendDataToServer("00000", CellID_Text.getText(),"" , "", "", "", "", "", false);
	}
});
btnPasif.setBounds(248, 292, 117, 25);
contentPane.add(btnPasif);

c1_Label = new JLabel("C1 :");
c1_Label.setBounds(10, 265, 70, 15);
contentPane.add(c1_Label);

C1_Text = new JTextField();
C1_Text.setColumns(10);
C1_Text.setBounds(83, 262, 59, 19);
```

```
contentPane.add(C1_Text);

C2_Label = new JLabel("C2 :");
C2_Label.setBounds(203, 262, 70, 15);
contentPane.add(C2_Label);

C2_Text = new JTextField();
C2_Text.setColumns(10);
C2_Text.setBounds(306, 262, 59, 19);
contentPane.add(C2_Text);

radio_btn_3G = new JRadioButton("3G BTS");
radio_btn_3G.setBounds(200, 185, 77, 23);
contentPane.add(radio_btn_3G);

radioBtnServing = new JRadioButton("Serving");
        radioBtnServing.setBounds(306, 185, 83, 23);
        contentPane.add(radioBtnServing);
}

private void SendDataToServer(String Code, String CellID_Text, String LAC_Text,
                String NCell_ID_Text, String MNC_Text, String MCC_Text, String
C1_Text,String C2_Text,Boolean radio_btn) {
        Socket clientSocket;
        try {
                clientSocket = new Socket(SERVER_IP, SERVERPORT );
                DataOutputStream outToServer = new
DataOutputStream(clientSocket.getOutputStream());

                String outString = Code + "," + CellID_Text  + "," + LAC_Text + "," +
NCell_ID_Text + "," +  MNC_Text + "," +
 MCC_Text + "," +  C1_Text + "," + C2_Text + "," + radio_btn.toString();

 outToServer.writeBytes( outString );
//                      clientSocket.close();

} catch (UnknownHostException e) {
        // TODO Auto-generated catch block
        e.printStackTrace();
} catch (IOException e) {
        // TODO Auto-generated catch block
                e.printStackTrace();
        }

}
private class SwingAction extends AbstractAction {
        public SwingAction() {
                putValue(NAME, "AKTIF");
putValue(SHORT_DESCRIPTION, "Some short description");
                }
                public void actionPerformed(ActionEvent e) {
                }
        }
```

ÖZGEÇMİŞ

Adı Soyadı : Ömer Faruk ÇELİK

Doğum Yeri : Muş

Doğum Tarihi : 14.12.1987

Medeni Hali : Evli

Yabancı Dili : İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise : Gaziantep Kolej Vakfı FEN Lisesi 2001-2004

Lisans : Orta Doğu Teknik Üniversitesi Bilgisayar Mühendisliği, 2004-2009

Yüksek Lisans : Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Eylül 2010- Şubat 2015

Yayınları:

1) Samet, R.**, Çelik, Ö.,F.** Sahte Baz İstasyonu Saldırı Tespit Algoritması, Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi. **İNCELEME AŞAMASINDA**

Kongre

1) **Çelik, Ö,F.**,Samet, R., 2014. Sahte Baz İstasyonu Saldırı Tespit Algoritması, 7th International Conference on Information Security and Cryptology (ISCTurkey 2014), 17-18 November, IscTurkey Proceding Book, 34-39, İstanbul.